Information & Computer Security

Explaining small business InfoSec posture using social theories

Eli Rohn Gilad Sabari Guy Leshem

Explaining small business infosec posture using social theories

INTRODUCTION

Sociologists and Economists recognize that business size, in terms of number of employees and revenue, creates create different classes of businesses and thus separate them into size clusters. Government agencies have been doing the same; developed countries have some form of a small business agency, e.g., The Small business Administration (SBA) in the US and Growth Hubs in England. Small businesses (SB) are studied and treated differently from larger businesses.

The importance of SB to the economy is undeniable (Nazar, 2013; European Commission, 2016), so it is therefore vital to protect this sector of the economy from cyber-attacks (Feagin, 2015; Kissel, 2009; Shoemaker et al., 2016).. The EU Commission, individual EU countries and many federal and state agencies in the USA invest immense financial resources in the form of tax payer's money to educate small businesses about cybersecurity (GOV.UK, 2016; SBA, 2013a; SBA, 2013b; SBA, 2016). Yet the situation is grim, as demonstrated in the current paper. There are plenty of news reports that scare SB owners and no shortage of government resources to help remedy the situation. So why is SB cybersecurity posture still so dismal? Bad management and lack of technical skills have not provided adequate explanation. Hence, we use social theories to explain the situation and provide recommendations that are practical and useful.

Our goal is to investigate information technology (IT) security practices of very small enterprises (ten to fifty employees) in various sectors using Israel, an OECD member state whose cyberspace has been frequently attacked, as a source for sample data and through that assess the country's SB information security posture. The resulting information is valuable not only to the research community, but also to managers and policy makers who strive to reduce information security vulnerability on local and national levels. For example, providing tax benefits to expenses related to information security fortification could motivate enterprise owners and managers to invest in improving their information security posture.

This article's contributions are threefold: first, the data was collected by direct observation and testing in the field, as opposed to relying on self-administered questionnaires. Second, inferential statistics were used to analyze the data collected. Third, an explanation of the results using theories of behavior from social science is offered, where social comparison theory and reliance on small samples play a key role.

The remainder of the article is organized as follows: a review of pertinent literature, which is then followed by an explanation and justification of the methodology used to collect data in the field. A report on results using descriptive statistics is given, followed by various hypothesis analyzed using inferential statistics, which are discussed in the following section. A summary and possible future research concludes the paper.

LITERATURE REVIEW

SB rely on information systems no less than large corporations do. Therefore, protecting their IT assets is as important to SB's as it is to large organizations.

Small business information security

Information security is a pervasive concern for all organizations (Gupta and Hammond, 2005). According to the Institute for Business and Home Safety, an estimated 25 percent of SB do not reopen following a major disaster (SBA, 2013a).

According to the US Small Business Administration (SBA), thirty one percent of all US cyber-attacks in 2012 targeted SB's. Many SB owners that run a large part of their business over the Internet do so without any information security features (Montgomery, 2013). A Forbes Magazine report on 2012 data breach investigations study by Verizon shows that in 855 data breaches Verizon examined, the majority (71 percent) occurred in businesses with fewer than 100 employees. Verizon's 2013 report shows attacks on SB's increasing in record numbers (Conner, 2013). Entrepreneur Magazine reported that "Cybercrime costs the economy more than $1 trillion per year, and crooks are increasingly setting their sights on small businesses" (Chickovski, 2010). Predictions, since the year 2000, that cyber-activists, hackers and terrorist groups will target ill-secured (soft) Internet-based quarries (Valeri and Knights, 2000) , have materialized in numerous occasions.

Even SB's that do not run a large part of their business over the Internet rely on IT to manage their affairs just as much as large enterprises (Newman, 2010; Chao and Chandra, 2012). From the literature, it is unclear if they place measures to mitigate risks arising from usage of IT, at the governance, management and technology levels. It is clear, however, that small organizations do fall victim to information security breaches.

Lay users find it difficult to understand and to use security aspects of software placed before them (Furnell et al., 2006). Usability of security features has not improved much (Furnell, 2007) and therefore the usability barrier still has a significant negative impact on end users who also own and operate SB's.

Lancaster University published a “Small Business Cyber Security Survey 2012” (Prince and King, 2012), whose aim was to gain a better understanding of how IT security in SB is being addressed. Data were collected using a survey administered to forty eight SB representatives who attended an information security conference. Because attending an information security conference does not attract a statistical random sample of the business population at large, its finding are even more telling, as it primarily includes tell those businesses that do care, at least to a degree, about information security. About seventy percent of businesses suffered from the consequences of malicious software attack. About eighty percent experienced a staff-related security incident. However, one must be careful not to assume that the consequence were grave.

The British Department for Business Innovation and Skills published a "2014 information security breaches survey" (BDBI, 2014). Based on data that was collected using a survey, sixty percent of SB’s had a security breach. Forty five percent of SB’s suffered from infection from viruses or malicious software in the prior year. Thirty three percent of SB’s were attacked by an unauthorized outsider in the prior year. Twenty two percent of SB’s suffered staff-related security breaches.

A recent survey conducted by a US leading SB insurer, Nationwide, found similar results in the USA (Poll, 2015). According to this report, a majority of them (sixty three percent) have been victims of at least one type of cyber-attack and almost eight in 10 SB owners (seventy nine percent) do not have a cyber-attack response plan.

These findings, spanning from 2012 to 2015 use similar surveys and have comparable findings, which suggests that despite large variety of SB size and locations, information security weakness is a shared characteristic. However, they do not explain why, both from a control perspective and a social perspective.

Fentz et. al. identified information security challenges for SB’s based on literature reviews and industry feedback such as the following: asset and countermeasure inventory; asset value assignment; risk prediction, the overconfidence effect; knowledge sharing and risk vs. cost trade-offs. However, unlike this article, their findings cannot be operationalized, according to the authors, nor are they explained theoretically (Fenz et al., 2014).

The Endurance International Group reported in 2015 that ninety five percent of their survey respondents admitted to having no information security insurance. Eighty three percent of SB owners handle their own information security matters, and do not have IT staff or utilize an outside resource (EIG, 2015).

Why the gap?

Theoretical explanations and some empirical data from tests have been proposed to help explain various aspects of this knowledge-action gap. However, most of these studies have suffered from a variety of methodological weaknesses including non-randomization, low response rates, localization, confusing formative with reflective analyses, reliance on purely self-reported data (Siponen et al., 2006; Siponen and Iivari, 2006; Prince and King, 2013) or a single case study (Heier and Garrett, 2014).

Addressing the knowing-doing gap problem in security breaches using behavioral interventions include punishment (Straub and Welke, 1998), instruction (Puhakainen and Siponen, 2010), organizational culture changes (Hu et al., 2012) and raising security awareness (Bullée et al., 2015; Tsohou et al., 2015). Regardless, SB's often fail to take basic security precautions that frequently result in significant losses. It has even been found that when people lack the skills necessary to utilize security technology and say they are willing to pay a fee to have their information protected, they often do not take advantage of this opportunity to improve their system security (Leyden, 2004). Although knowledge of cybersecurity related behavior has improved in recent years, "knowing better, but not doing better" remains a scholarly and practical issues to be understood. The current paper addresses this fundamental problem by utilizing two social theories: social comparison and rare events bias, a novel approach that has not been reported in the literature.

Social Theories

Social Comparison is an idea that concerns the appraisal and evaluations of abilities, as well as opinions, of oneself (Festinger, 1954). There is empirical evidence that humans have a drive to evaluate their opinions and their abilities and the evidence indicates that the two are closely linked and affect behavior. "The holding of incorrect opinions and / or inaccurate appraisals of one's abilities can be punishing or even fatal in many situations" (Festinger, 1954). According to the theory, humans determine their own social and personal worth based on how they stack up against others. As a result, humans are constantly making self and other evaluations across a variety of domains.

Humans compare their abilities in several ways, including competition, cooperation, and conformity. It has been found that the degree of interpersonal similarity among group members influences competition and cooperation (Miller and McFarland, 1991).

Additionally, humans have a tendency to assess risks in a non-objective manner, leading to optimistic bias (Weinstein and Klein, 1996). In the context of information security, a 2004 survey (AOL/NCSA, 2004) supported this tendency of underestimation of one’s own risk. The hypothesis that IT executives have an optimistic bias in their risk perception related to their firms’ information security has been shown to be valid, based on a mailed survey (Rhee et al., 2012). The same can be said about the hypothesis that IT executives perceive their organizations to have a higher degree of controllability for their organizations’ information security than other organizations (Rhee et al., 2012). The same research reports on unjustified optimism of managers about their SB information security posture. They find that increased vulnerability to information security breaches is coupled with low levels of managerial awareness and commitment regarding information security threats and term this dissonance optimistic bias. According to social comparison theory (Festinger, 1954), people seek to evaluate their standings and opinions and abilities; they prefer objective measures, but in their absence people compare themselves to other people. “One does not evaluate the correctness of an opinion by comparison with others whose opinions are extremely divergent from one's own. Given a range of possible persons for comparison, someone close to one's ability or opinion will be chosen for comparison” (Festinger, 1954).Social referents and network structures influence judgments about the importance of certain knowledge (Wong, 2008). Opinions and abilities, as manifested through performance or illusion of performance, act together in the manner they affect behavior. A person's opinions and beliefs about self and one’s given situation greatly influence the person's behavior. Holding incorrect opinions and/or inaccurate appraisal of one's abilities can be punishing, even deadly (Festinger, 1954). More recent research shows that these comparisons have an inherent bias: most people believe that they are less likely to experience a negative event and more likely to experience a positive event than their referents. This bias also exists in groups (Rhee et al., 2012). To that, one can add an assertion made by Kahneman and Tversky (1979): “because people are limited in their ability to comprehend and evaluate extreme probabilities, highly unlikely events are either neglected or overweighed". Follow-up contemporary studies have shown that people made choices as if they underweighted rare events; that is, rare events received less weight than their objective probability of occurrence warranted (Yechiam et al., 2005; Hertwig et al., 2004; Hertwig and Erev, 2009). When people can rely solely on self-experience with risky prospects, then they underweight the probability of rare events, leading to an erroneous understanding of the environment in which they operate. Reliance on small samples of experience contributes to the perception of the world as less variable than it actually is (Hertwig and Erev, 2009).

Risk management

A control is a measure intended to reduce risk to a level acceptable by management. IT internal controls at a governance level involve ensuring that effective IT management and security principles, policies, and processes with appropriate compliance measurement tools to assess and measure those controls, are in place and operate effectively. At the management level, controls include usage of and adherence to IT standards, the creation, maintenance and re-certification of formal organizational structures, work related procedures, physical and environmental control directives, and more. The technology level in the hierarchy has two types of general controls: systems software and systems development general controls, followed by application-based controls.

Of the several information security frameworks available in the market, we use Control Objectives for IT (COBIT) because it strongly connects between business goals and technological means to achieve them and it is updated regularly. Further, COBIT is concise, compared, for example, to the very detailed ISO27000 family of standards, or the NIST-800 framework, whose coverage includes national critical infrastructure to Post-Quantum Cryptography. NISTIR 7621 (Small Business Information Security - The Fundamentals) has not been updated since 2009 (Kissel, 2009) and its principles overlap those of COBIT. Additionally, COBIT is recognized by the American governing body, the Public Company Accounting Oversight Board (PCAOB), and is applicable even to SB's, including those traded in a US exchange thus subjected to Sarbanes-Oxley regulations. COBIT accommodates new and revised guidance from the PCAOB, the AICPA's (the American Institute of Certified Public Accountants) Auditing Standards Board (ASB) and the COSO's (Committee of Sponsoring Organizations of the Treadway Commission) revised edition of its Internal Control Framework. These contributions and recognitions make COBIT a very strong framework for cybersecurity posture evaluation.

COBIT is a set of IT controls and best practices that we used in our data collection and evaluation. It is a framework created by the Information Systems Audit and Control Association (ISACA) for IT management and IT governance. COBIT is an internationally accepted guide for IT governance (ISACA, 2013). Version 4.1 that was used in this research defines IT activities in a generic process model within four domains, which are the following: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). PO provides direction to solution delivery (AI) and service delivery (DS). AI provides the solutions and passes them to be turned into services. DS receives the solutions and makes them usable for end users. ME monitors all processes to ensure that the direction provided is followed. Altogether, there are thirty four IT processes within these four domains. The fifth section in COBIT's Deliver and Support chapter, titled *Ensure Systems Security*, has several processes that provide information security guidance for management and IT professionals. The section helps understand, utilize, implement and direct key information security related activities. It addresses IT risk management by providing guidelines on how to achieve or improve confidentiality, integrity, availability and privacy of data and IT systems. The current study heavily utilized this research. However, information security does not work in isolation. The topic appears in all four COBIT domains starting with proper planning and organizing (PO), followed by acquisition of information security means and measures (AI), which forms the basis for implementation and ongoing support (DS). Details appear in appendix A.

ISACA included in version 4.1 of COBIT a Maturity Model (Table 1) based on the Capability Maturity Model (CMM). It is used to measure how well developed management processes are with respect to IT internal controls.

[INSERT TABLE 1 HERE]

METHODOLOGY

Information security surveys are usually over-optimistic and avoid admission of guilt, yielding results that are less accurate than field work (Shah, 2015; BITSIGHT, 2015; Bradley, 1981). This is why professional auditors conduct most of their work at client sites rather than process a questionnaire (PCAOB, 2003; IIA, 2003; AICPA, 2015). Therefore, we used the field research approach to gather qualitative and quantitative data in active organizations, in alignment with the book *Essentials of Business Research Methods* (Hair et al., 2015). This approach requires the researcher to "go into the field" to observe the phenomenon in its natural state or in situ. The field researcher typically takes extensive field notes that are subsequently coded and analyzed in a variety of ways. An audit is in fact a field investigation: auditors observe people and processes, review papers and other artifacts, and use semi-structured interview techniques to obtain additional data pertinent to the audit's stated goal and scope. The current paper utilized COBIT as the "golden standard" for reasons explained in the literature review.

Research Design and Execution

The data for this study had been collected by performing actual information security audits at SB's by fourth year information technology students in two research universities. These well-trained and closely supervised students collected audit related data at least as well as accountants who are fresh out of college, have no IT background and are assigned to IT audits as data collectors by reputable professional service providers such as KPMG, Ernst & Young, BDO and others. The effort spanned about twenty four months. Students performed the audit work as part of a semester-long assignment given to them in an IT Audit and Assurance course. The assignment addressed IT security from a human-centric perspective rather than a technology-centric perspective. Given that over half of all information systems security breaches are caused by employees failing to comply with procedures, it is particularly important for organizations to address non-technical dimensions of information security, such as legal aspects and human behavior perspectives (Ahmad and Maynard, 2014).

[INSERT FIGURE 1 HERE]

This field study had several stages, in accordance to IT Audit best practices (Figure 1). First, the scope and goal of the audit were defined in writing. Then students formed groups of four who had several distinct responsibilities: group manager, audit report writer and two students to perform the field work. Their first task was to find a "client" using their social networks or via cold-calling techniques, asking the recipient to participate in a research (not an audit) on information security. Then they proceeded to formulate an engagement letter, create a risk matrix (Figure 2) and a pertinent test matrix outlining verification methods for each risk that the organization claims it addresses. The risk and test matrixes focused on information security, yet allowed for additional topics. Once the matrixes were approved by a certified IT auditor (CISA), students performed the field work: review documents, observe people and processes, and interview management and technical staff. All evidence gathered along with supporting work papers were recorded and saved. Lastly, each group wrote an audit report, delivered a copy to their client organizations and discussed it with management in a closing meeting.

[INSERT FIGURE 2 HERE]

Each deliverable was reviewed by a CISA who provided professional audit services for a decade and a teacher assistant with prior experience in IT audit. The reviews focused on quality and adherence to professional practices. Non-satisfactory deliverables had to be re-worked once and even twice, including follow-up visits to clients. Each re-work was reviewed again by the CISA and the teacher assistant. Students were instructed to collect specific data using a prescribed collection method. The students, under the supervision of the

CISA, evaluated each control if it provides adequate means to reduce specific risks. For well-designed controls, the students and the CISA evaluated if the control operates as expected, assigning each such control one of three mutually exclusive options: operates as expected, operates partially, and does not operate as expected. All students had to present their findings to the entire class. This provided an opportunity the researchers and for other students to inquire about their work and impressions.

The participating SB's were chosen randomly; they belong to a variety of economy sectors and geographical locations, which ensured a valid representative random sample. That is, the sample replicate as closely as possible elements of the larger population under study. "The literature on numerical approaches to quantify information-security risk is scarce" (Patel et al., 2008). Therefore the study focused on analyzing the results using inferential statistical methods in addition to qualitative ones.

RESULTS

17 organizations participated in this study. Twenty seven students from the northern university visited nine (fifty three percent) organizations; thirty two students from the southern university visited eight (forty seven percent) organizations. Six organizations (thirty five percent) were from the southern part of the state, the other eleven (sixty five percent) from its northern part (Figure 3). Most clients were visited in their premises twice during the data collection phase, each visit lasting between three and four hours. Four clients required a third short visit. Overall, 206 (100 percent) tests were carried out. The most frequent controls tested are listed, along with their description, in Appendix A.

[INSERT FIGURE 3 HERE]

[INSERT TABLE 2 HERE]

Only about one third of *all* the controls examined were designed properly and operated as expected. About half of the controls were either ill-designed or did not operate as intended. Non-profit organizations were more at risk than for-profit ones (Figure 4).

[INSERT FIGURE 4 HERE]

Plan and Organize (PO) had thirty seven controls, of which more than half failed. Acquire and Implement (AI) had thirty one controls, of which about one third failed. Deliver and Support (DS) had 124 controls, almost half of which failed. Monitor and Evaluate (ME) had fourteen controls, of which more than half failed.

Only one organization has a defined strategic IT plan (PO1), and it was found to be inadequate. Thus SB's have a failure rate of 100 percent for this control. Only seven organizations have formally defined the information architecture (PO2), and of these five (seventy one percent) failed to do it properly. None has given formal thought for defining their technological direction (PO3). However, all organizations have defined, at least to some degree, their IT processes and relations to business processes (PO4). Managing the IT investment (PO5) was not a control this study considered. All SB's partially communicate management's aims and direction (PO6) pertaining to IT. Management of IT human resources (PO7) is generally dichotomous, either done or not done, with few exceptions. Quality management of IT processes (PO8) was not a control examined in this study. An overwhelming majority of SB's do not assess and manage IT risks (PO9).

The Acquire and Implement (AI) controls were not part of the controls students were required to evaluate; the few data items we have were observed and evaluated voluntarily. This small number of observations precludes the possibility that this data are representative of anything. However, controls over the design of the applications and the proper inclusion of application controls and security requirements (AI2) have been evaluated for eleven SB organizations, and found to be inappropriately carried out by most of them.

The study collected data for several controls within the Deliver and Support (DS) cluster. Controls ensuring effective third-party management process (DS2) are in place in virtually all organizations and for the vast majority the controls operate as intended. There are well defined roles, responsibilities and expectations relating to third-party agreements. Controls of performance and capacity of IT (DS3) were not included in the audit's scope. Most SB's do not invest in ensuring continuous service (DS4). Therefore, most SB's are exposed to the impact of a major IT service interruption on key business functions and processes. Only about one third of SB's have adequate mechanisms to ensure their IT security (DS5). These measures include user account management (although lax often times due to shared user accounts and due to simple, never expiring passwords) and anti-malware installation to protect against malicious software attacks. Identify and Allocate Costs (DS6) was not the audit's scope. The vast majority of SB's (seventy eight percent) do not invest educating and train users (DS7) in IT pertinent to their organization. Since SB visited do not have a help desk, the control Manage Service Desk (DS8) was omitted from the audit's scope, as were DS9 (Manage the Configuration) and DS10 (Manage Problems). Data management (DS11) is given some degree of attention by most SB's; thirty percent of SB failed this aspect entirely. Manage the Physical Environment (DS12), such as protecting against environmental factors and providing physical security for their servers and computers, is reasonably addressed by about half of SB's that had this control audited. Operations management (DS13) was omitted from the audit's scope.

Monitor and Evaluate (ME) controls were all out of scope for this audit. Five audit teams looked into them voluntary. The amount and quality of data obtained for this cluster precludes it from being considered representative.

The following two tables summarize the findings and provide the data for hypothesis testing described in the inferential statistics section.

[INSERT

Table ***3*** HERE]

[INSERT

Table 4 HERE]

Generally, students were amazed, surprised and sometimes shocked by their client's lack of knowledge about information security fundamentals and business continuity basics. Students reported lack of awareness and no familiarity with probabilities of being hit by an IT disaster, as well as almost complete ignorance of business survival probabilities. Claims such as "we've been X years in business, and it never happened to us therefore it won't in the future"; "it happens, but to others" faithfully describe impressions students received from SB owners and managers. Although Symantec, RSA, Kaspersky, Deloitte global security survey, Ernst & Young global information security survey, CSI/FBI computer crime and security survey, SANS institute, and many others publish periodically information security statistics (Dlamini et al., 2009), this information appears to be out of scope or inaccessible to very small organizations.

INFERENTIAL STATISTICS ANALYSIS

The study attempts to reach conclusions that extend beyond the immediate data alone using inferential statistics. Specifically, the study assesses the probability that observed differences between various data groups, if such exists, happened by chance in this study. For this purpose, the study categorized the data as follows:

- Technical versus Managerial controls
- North versus South physical location
- Service Providers versus Manufacturers
- Old versus Young organizations
- Private versus not for profit organizations

For each group we proposed a null hypothesis where there is no significant difference in performance, and posed an alternate hypothesis where there is a difference in performance. Each set of hypothesis was tested for variance equality (Levene, 1960) in order to accept or reject our assumption that the two groups of controls have homogeneous variance. If the variances were equal we used the T-Test to compare averages and assess if there is a statistically significant difference between the groups.

H1 Technical versus Managerial Controls

The study assumes that an environment that is notoriously weak in formal management would at least implement technical controls in a more competent manner, because such controls do not require as much organizational discipline. The study needed to verify or refute the assumption that technical controls would be implemented with greater competence compared to “softer” managerial controls. To that end, the study compared the two groups using raw data described earlier and repeated in **Error! Reference source not found.** providing an illustration for all statistical tests.

[INSERT

Table 5 HERE]

$H1_0$: Technical controls are implemented at the same competence level as managerial controls

$H1_1$: Technical controls are better implemented than managerial controls

T-Test results indicate there is no statistically significant difference between the implementation of controls between the two groups (0.687 > 0.05). Hence we have to accept $H1_0$ and accept the outcome that technical controls are implemented at the same competence level as managerial controls.

H2 Geographic Location

The study desired to learn if there is a difference in the level of information security between organizations from the country's north versus those from the south.

$H2_0$: Information security control are implemented at the same competence level in the north and south

$H2_1$: Information security control are implemented at different competence level in the north and south

T-Test results indicate there is no statistically significant difference between the implementation of controls between the two groups (0.558 > 0.05). Hence $H2_0$ cannot be rejected and one has to accept the outcome that organizations across the country implement information security controls at the same competence levels.

H3 Service Providers versus Manufacturers

Manufacturers by nature use engineering principles to create and operate their business. Therefore the study assumes that manufacturers will show higher competency in implementing at least the technical information security measures, thus exhibiting an advantage over service organizations.

$H3_0$: Information security control are implemented at the same competence level in the north and south

$H3_1$: Information security control are implemented at different competence level in the north and south

T-Test results indicate there is no statistically significant difference between the implementation of controls between the two groups (0.671 > 0.05). Hence $H3_0$ must be accepted, which leads to the conclusion that engineering practices did not cross over to IT.

H4 Old versus Young Organizations

The study defines young organizations as those that exist and operate five years or fewer. All others are considered mature. The study assumed that older organizations had time and resources to establish better habits and embrace best practices in information security, because they are not in a start-up frenzy mode of operation.

$H4_0$: Information security control is implemented at the same competence level in young and older organizations.

$H4_1$: Information security control is implemented at better competence level by older organizations.

T-Test results indicate there is no statistically significant difference between the implementation of controls between the two groups ($0.301 > 0.05$). Hence $H4_0$ must be accepted, which leads to the conclusion that organizational age has no impact on how information security is treated and implemented.

H5 Private versus not for Profit Organizations

The study assumed that private SB have more motivation to protect their IT assets and the business that relies on IT.

$H5_0$: Information security control is implemented at the same competence level in private and not for profit organizations.

$H5_1$: Information security control is implemented at better competence level by private organizations compared to not for profit organizations.

T-Test results indicate there is no statistically significant difference between the implementation of controls between the two groups ($0.610 > 0.05$). Hence $H5_0$ must be accepted, which leads to the conclusion that SB do not treat and implement information security differently than not for profit organizations.

H6 Implementers of Managerial Controls do better with Technical Controls

It was imperative for the study to verify or refute the assumption that organizations that implement both managerial and technical controls have their technical controls better implemented than those organizations who lack managerial controls (e.g., COBIT’s plan and organize).

$H6_0$: Technical controls are implemented at the same competence level by both groups.

$H6_1$: Technical controls are better implemented by organizations that also implement managerial controls.

T-Test results indicate there is no statistically significant difference between the implementation of controls between the two groups (0.985 > 0.05). Hence $H6_0$ must be accepted and the hypothesis that technical controls operate better in organizations implement both managerial and technical controls must be rejected.

DISCUSSION

The data had been collected by performing actual information security audits at small private businesses and small not for profit organizations. Therefore, the data reflects actual status, rather than self-reported status using a questionnaire (Bojanc and Jerman-Blažič, 2008; Whitman, 2004; Yeniman et al., 2011). The overall situation is grim: all organizations audited in the study do not have adequate information security controls, and if they do, many controls are either ill designed or not working as intended. This coincides with findings reported Yeniman et al. (2011) and by Laleh et al (2013). The level of maturity assessed using COBIT's CMMI (Table 1) is usually level one (initial /ad-hoc): there is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are no standardized processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management of IT security is disorganized. Often the organization has not even recognized that there is an issue to be addressed. As a result, these organizations are heavily exposed to various information security threats, including cyber-attacks and inside fraud. To make things worse, workers at all levels do not normally interact with information security software, such as anti-virus, firewall, intrusion detection systems and logs in the way that they do with websites or information systems, such as accounting or email. The cliché out of sight out of mind may hold some truth here.

Since the study uncovered no evidence that the low level of performance can be explained by any one of the six specific characteristics analyzed using qualitative and quantitative statistics, a plausible explanation must be found elsewhere. One possibility that comes to mind is a recent study by MIT Sloan Management Review and Cap Gemini Consulting (Fitzgerald et al., 2013). Thirty nine percent of the 1523 respondents agreed that the most significant organizational barrier to digital transformation in their organization was "lack of urgency". Is it because owners' knowledge of IT is lacking? Chao and Chandra (2012) have shown that knowledge of IT is a significant predictor of IT strategic alignment, as well as adoption of traditional IT and Internet technologies. Yet this doesn't explain why SB's do not invest in knowing more about IT, or hire someone that possess the required knowledge. A possible rational explanation is that these organizations find no utility in such an investment, regardless of whether or not their risk assessment is based on facts or wishful thinking. Another possibility is that the decision makers' access to pertinent information is lacking, and their personal experience, which they rely on, underweights the probability of rare events such as inside fraud or cyber-attack.

During the data collection phase, it was noted that managers use their own experience or that of a small number of other similar businesses they know. This small sample leads to an erroneous comprehension of their business environment as it relates to information security and continuity, manifesting a "rare events bias" (Hertwig et al., 2004; Hertwig and Erev, 2009; Yechiam et al., 2005). This bias can also explain the "lack of urgency" described earlier, which negatively impacts IT governance. Additionally, the general lack of easily accessible credible data about actual damages from information security in SB's on the one hand, and the interaction among SB's in their neighborhood (and sometimes in their associations) causes SB owners and managers to appraise their opinions and their abilities in relation to information security among themselves (social comparison). This further strengthens the sense that information security incidents are rare, thus there is no urgency and as a result fortifies the optimistic bias phenomenon. To sum up: technical and managerial characteristics cannot explain the high risk and lack of commensurate action to mitigate it among SB's. A social explanation combining rare events bias and social comparison is more plausible. Therefore, the study posits that improving the situation should start by addressing these two factors.

While an in-depth evaluation of specific means and their proper combination that will elevate SB awareness and reduce risk is beyond the scope of this research, the current study has raised two possibilities: moving IT operations to a managed cloud environment has the potential to reduce information security risks. However, such a move requires SB owners to understand the option. Tax incentives could provide the needed motivation to invest in information security and thus reduce pertinent risks to a large sector that is vital for a healthy economy.

SUMMARY

SB's and small not for profit organizations rely on IT to operate and manage their outfits. This exposes them to risks stemming out of the mere usage of the technology. Specifically, they are more exposed than ever before to information security risks. These could be internal fraud or attacks that are launched from outside the organization. Managing these risks requires the organization to use a solid framework for establishing, maintaining and updating risk mitigating controls. COBIT is one such framework the current study used to convey information security evaluation in small organizations. The study's field work examined seventeen different small organizations selected at random. Overall, 206 tests were carried out. The top three controls tested were DS5.3 (Identity Management), DS5.9 (Malicious Software Prevention, Detection and Correction) and DS5.4 (User Account Management). Approximately one third of all the controls examined were designed properly and operated as expected. About half of the controls were either ill-designed or did not operate as intended. A plausible explanation to the low levels of performance witnessed and measured in the study is the rare events bias, which leads to risk underestimation and therefore a lack of urgency to invest in information security such that it will match risks and the business risk appetite. SB owners and C-level managers are advised to learn more about information security and implement free or low cost measures to better protect their financial interests. These stakeholders would benefit from effective implementation of weak or non-existing controls. The findings reported here could serve as a good starting point. These stakeholders have an interest in ensuring the viability of their outfits and the provision of goods and services under adverse conditions. Concerns about the return on security investments that may not yield immediately measureable benefits could be mitigated by effective tax incentives to help justify the costs of improved information security, by balancing the short-term costs of additional investment with similarly near-term benefits. Governments have an obligation to ensure the economy operates reasonably well under cyber-attacks and thus has the legitimacy and the incentive to offer tax breaks to small outfits would otherwise remain vulnerable even if their management is aware of the need to be cyber-resilient. Designing and implementing such tax incentives is left for economists and finance mavens to research and recommend. Further, governments may want to launch an awareness campaign encouraging small outfit stakeholders to learn more about information security and about offered tax breaks. A repeat of a similar research after the implementation of such means would measure the effectiveness of these proposals and more importantly, find out if this sector of the economy indeed became more secure and resilient to cyber-attacks.

REFERENCES

Ahmad A and Maynard S. (2014) Teaching information security management: reflections and experiences. *Information Management & Computer Security* 22: 513-536.

AICPA. (2015) AICPA Standards and Statements In: CPAs AIo (ed). New York, New York: American Institute of CPAs.

AOL/NCSA. (2004) AOL/NCSA online safety study. Research Report, American Online and the National Cyber Security Alliance. *available on* http://tinyurl.com/oqpgrjw.

BDBI. (2014) information security breaches survey, 2014. United Kingdom: The British Department for Business Innovation and Skills.

BITSIGHT. (2015) Cyber Security Myths Versus Reality: How Optimism Bias Contributes to Inaccurate Perceptions of Risk. Dimentional Research, 8.

Bojanc R and Jerman-Blažič B. (2008) An economic modelling approach to information security risk management. *International Journal of Information Management* 28: 413-422.

Bradley JV. (1981) Overconfidence in ignorant experts *Bulletin of the Psychonomic Society* 17: 82-84.

Bullée J-WH, Montoya L, Pieters W, et al. (2015) The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology* 11: 97-115.

Chao C-A and Chandra A. (2012) Impact of owner's knowledge of information technology (IT) on strategic alignment and IT adoption in US small firms. *Journal of Small Business and Enterprise Development* 19.

Chickovski E. (2010) *Protect Your Small Business Against Cyber Attacks*. Available at: http://www.entrepreneur.com/article/206656.

Conner C. (2013) *Record Number Of Cyber Attacks Target Small Business*. Available at: http://tinyurl.com/CyberSecVZ.

Dlamini MT, Eloff JHP and Eloff MM. (2009) Information security: The moving target. *Computers & Security* 28: 189-198.

EIG. (2015) *A Vast Majority of U.S. Small Business Owners Believe Cybersecurity Is a Concern*. Available at: http://tinyurl.com/q6tn2mz.

European Commission. (2016) *What is an SME?* Available at: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm.

Feagin RD. (2015) The value of cyber security in small business. Utica College, 45.

Fenz S, Heurix J, Neubauer T, et al. (2014) Current challenges in information security risk management. *Information Management & Computer Security* 22: 410-430.

Festinger L. (1954) A Theory of Social Comparison Processes. *Human Relations* 7: 117-140.

Fitzgerald M, Kruschwitz N, Bonnet D, et al. (2013) Embracing Digital Technology. *MIT Sloan Management Review*. MIT Sloan School of Management.

Furnell S. (2007) Making security usable: Are things improving? *Computers & Security* 26: 434-443.

Furnell S, Jusoh A and Katsabas D. (2006) The challenges of understanding and using security: A survey of end-users. *Computers & Security* 25: 27-35.

GOV.UK. (2016) *OCSIA supporting education, awareness and training*. Available at: http://tinyurl.com/UKcyber01.

Gupta A and Hammond R. (2005) Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security* 13: 297-310.

Hair J, Joseph F. , Wolfinbarger M, Money AH, et al. (2015) *Essentials of Business Research Methods,* New York, NY: Routledge.

Heier DA and Garrett GW. (2014) Evaluating Results of a Small Business Security Survey. In: Bhargava V and Swaraj A (eds) *Proceedings of the Society of Business, Industry and Economics 2014 Conference.* Destin, Florida: Society of Business, Industry and Economics, 34-45.

Hertwig R, Barron G, Weber EU, et al. (2004) Decisions from Experience and the Effect of Rare Events in Risky Choice. *Psychological Science* 15: 534-539.

Hertwig R and Erev I. (2009) The description–experience gap in risky choice. *Trends in Cognitive Sciences* 13: 517-523.

Hu Q, Dinev T, Hart P, et al. (2012) Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences* 43: 615-660.

IIA. (2003) IIA International Professional Practices Framework for Auditors. In: Auditors TIoI (ed). Altamonte Springs, FL: The Istitute of Internal Auditors.

ISACA. (2013) *COBIT 4.1: Framework for IT Governance and Control*. Available at: http://tinyurl.com/cobit41z.

Kahenman D and Tversky A. (1979) An Analysis of Decision under Risk. *Econometrica* 47: 263–291.

Kissel R. (2009) NISTIR 7621: Small Business Information Security - The Fundamentals. In: Commerce Do (ed). US Government.

Laleh E, Masoudi Y, Fathy F, et al. (2013) Influencing Factors of Information Security Management in Small- and Medium-Sized Enterprises and Organizations. *Communication Systems and Network Technologies (CSNT), 2013 International Conference on.* 445-449.

Levene H. (1960) In: eds IOea (ed) *Contributions to Probability and Statistics: Essays in Honor of Harold Hotelling.* Stanford University Press.

Leyden J. (2004) *Clueless office workers help spread computer viruses*. Available at: http://www.theregister.co.uk/2004/02/06/clueless_office_workers_help_spread/.

Miller DT and McFarland C. (1991) When social comparison goes awry: The case of pluralistic ignorance. In: Wills JSTA (ed) *Social comparison: Contemporary theory and research.* Hillsdale, NJ, England: Lawrence Erlbaum Associates, Inc, 287-313.

Montgomery T. (2013) *Do Small Businesses Need to Worry About Cyber Security?* Available at: http://tinyurl.com/ojl4equ.

Nazar J. (2013) 16 Surprising Statistics About Small Businesses. *Forbes.*

Newman P. (2010) Evaluating the effect of information technology in small businesses. *PhD Dissertation at the School f Business and Technology.* Minneapolis, MN, USA: Doctoral Dissertation, Capella University, 161.

Patel SC, Graham JH and Ralston PAS. (2008) Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management* 28: 483-491.

PCAOB. (2003) PCAOB Auditing and Related Professional Practice Standards. In: Board PCAO (ed) *Section 3.*

Poll H. (2015) *Nationwide Cyber Security Survey*. Available at: http://tinyurl.com/Nationwide2015.

Prince D and King N. (2012) Small Business Cyber Security Survey 2012. Lancaster University, 38.

Prince D and King N. (2013) Small Business: Cyber Security Survey 2012. Lancaster University,.

Puhakainen P and Siponen M. (2010) Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly* 34: 757-778.

Rhee H-S, Ryu YU and Kim C-T. (2012) Unrealistic optimism on information security management. *Computers & Security* 31: 221-232.

SBA. (2013a) *Disaster Planning*. Available at: https://www.sba.gov/content/disaster-planning.

SBA. (2013b) *Do Small Businesses Need to Worry About Cyber Security?* Available at: http://tinyurl.com/SBAcyber02.

SBA. (2016) *Cybersecurity for Small Businesses*. Available at: http://tinyurl.com/SBAcyber01.

Shah S. (2015) *Cyber Security Risk: Perception vs. Reality in Corporate America*. Available at: http://tinyurl.com/BITSIGHT2013.

Shoemaker D, Kohnke A and Sigler K. (2016) *A Guide to the National Initiative for Cybersecurity Education,* Boca Raton, FL: CRC PRess.

Siponen M and Iivari J. (2006) IS security design theory framework and six approaches to the application of IS security policies and guidelines. *Journal of the Association for Information Systems* 7: 445–472.

Siponen M, Pahnila S and Mahmood A. (2006) Factors influencing protection motivation and IS security policy compliance. *Innovations in Information Technology* November.

Straub DW and Welke RJ. (1998) Coping with systems risk: Security planning models for management decision making. *MIS Quarterly* 22: 441–469.

Tsohou A, Karyda M, Kokolakis S, et al. (2015) Managing the introduction of information security awareness programmes in organisations. *Eur J Inf Syst* 24: 38-58.

Valeri L and Knights M. (2000) Affecting Trust: Terrorism, Internet and Offensive Information Warfare. *Terrorism and Political Violence* 12: 15-36.

Weinstein, N.D and Klein WM. (1996) Unrealistic optimism: present and future. *Journal of Social and Clinical Psychology* 15: 1-8.

Whitman ME. (2004) In defense of the realm: understanding the threats to information security. *International Journal of Information Management* 24: 43-57.

Wong S-S. (2008) Judgments about knowledge importance: The roles of social referents and network structure. *Human Relations* 61: 1565-1591.

Yechiam E, Barron G and Erev I. (2005) The Role of Personal Experience in Contributing to Different Patterns of Response to Rare Terrorist Attacks. *Journal of Conflict Resolution* 49: 430-439.

Yeniman YE, Akalp G, Aytac S, et al. (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management* 31: 360-365.

Author Biographies

Eli Rohn holds a PhD in Information Systems from NJIT. He is a faculty member with the department of information systems engineering at Ben-Gurion University of the Negev. His research interests include complex adaptive systems, audit and information security.

Gilad Sabari holds a Bsc in software engineering from the department of information systems engineering at Ben-Gurion University of the Negev. He is pursuing his Masters' degree at the same place. His research interests include cybernetics and cyber-security.

Guy Leshem holds a PhD in Statistics from the Hebrew University, Jerusalem. During the development of this manuscript he was a post-doctoral student with the department of computer science at Ben-Gurion University of the Negev. His research interests include Statistical learning theory; Polynomial time algorithms; Communication networks and game theory.

BGU is ranked 30th worldwide among universities that are less than 50 years old on the QS World University Rankings 2014/2015 report.

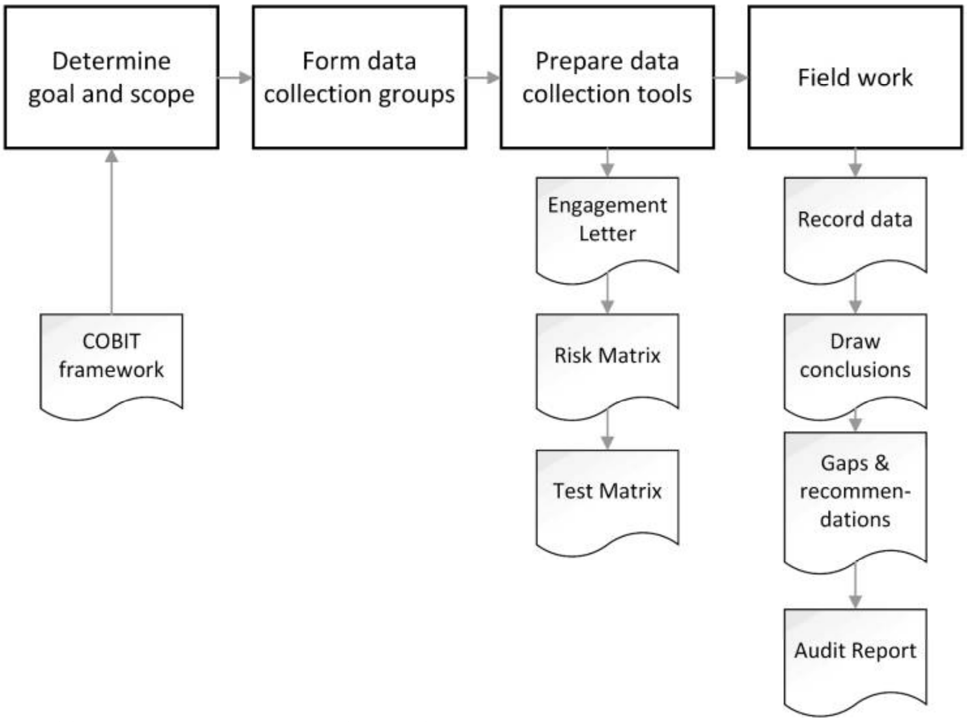
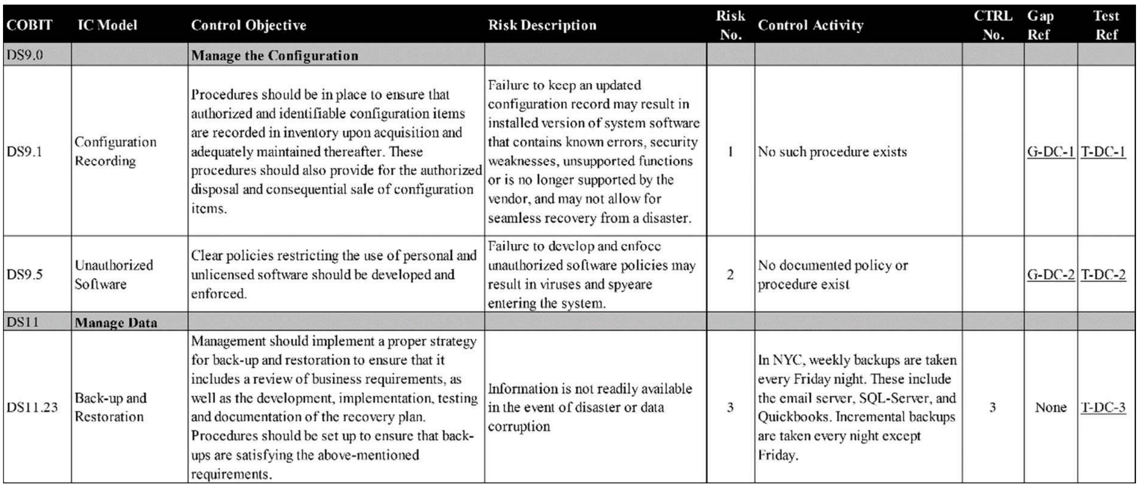


Figure 1: Field Experiment Process Based on Audit Best Practice



COBIT	IC Model	Control Objective	Risk Description	Risk No.	Control Activity	CTRL No.	Gap Ref	Test Ref
DS9.0		**Manage the Configuration**						
DS9.1	Configuration Recording	Procedures should be in place to ensure that authorized and identifiable configuration items are recorded in inventory upon acquisition and adequately maintained thereafter. These procedures should also provide for the authorized disposal and consequential sale of configuration items.	Failure to keep an updated configuration record may result in installed version of system software that contains known errors, security weaknesses, unsupported functions or is no longer supported by the vendor, and may not allow for seamless recovery from a disaster.	1	No such procedure exists		G-DC-1	T-DC-1
DS9.5	Unauthorized Software	Clear policies restricting the use of personal and unlicensed software should be developed and enforced.	Failure to develop and enfoce unauthorized software policies may result in viruses and spyeare entering the system.	2	No documented policy or procedure exist		G-DC-2	T-DC-2
DS11	**Manage Data**							
DS11.23	Back-up and Restoration	Management should implement a proper strategy for back-up and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Procedures should be set up to ensure that back-ups are satisfying the above-mentioned requirements.	Information is not readily available in the event of disaster or data corruption	3	In NYC, weekly backups are taken every Friday night. These include the email server, SQL-Server, and Quickbooks. Incremental backups are taken every night except Friday.	3	None	T-DC-3

Figure 2: Risk Matrix

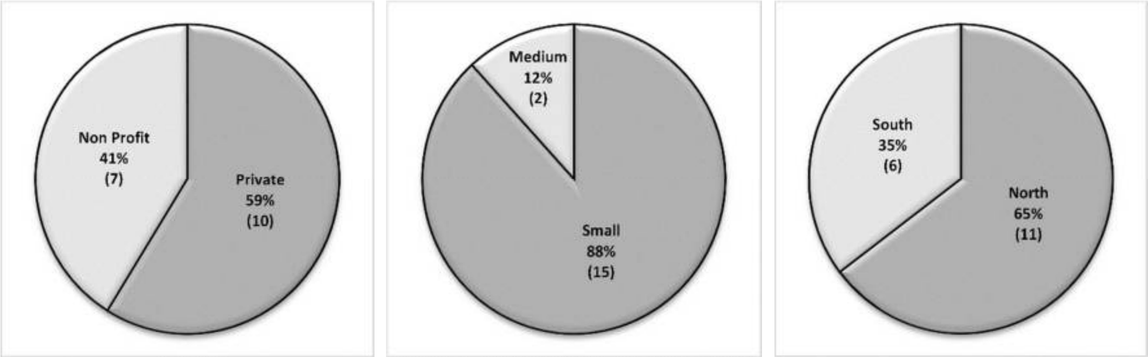


Figure 3: Division of Organizations by type, size and location. Results presented in percentage and number of organizations

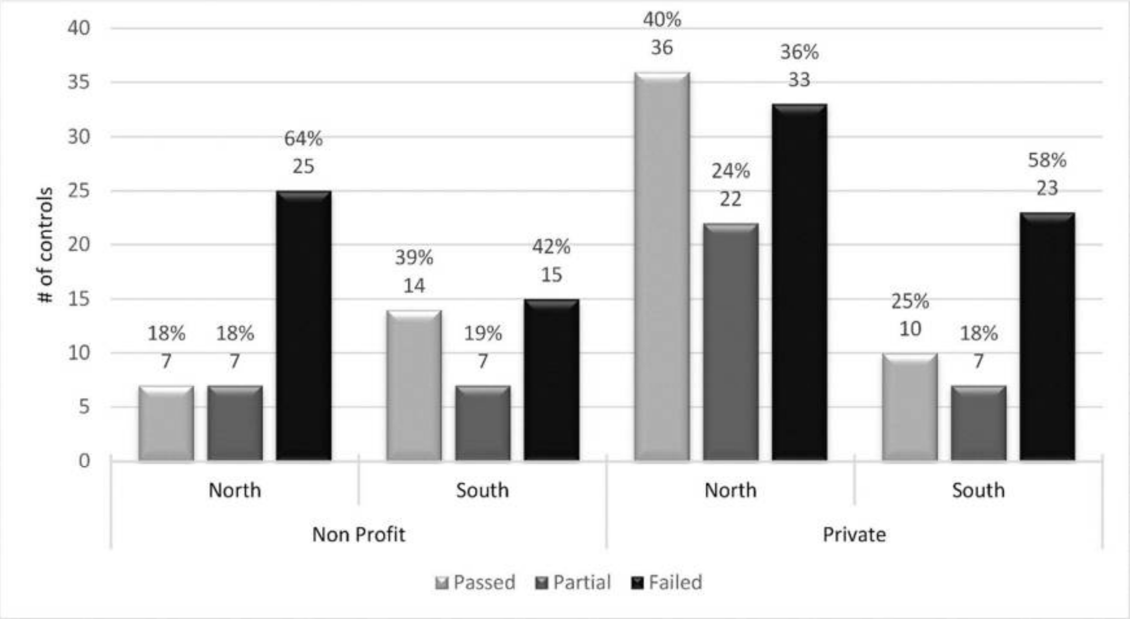


Figure 4: Controls Disposition: Pass, Fail, Partial. First division by type of organization and subdivision by location. Results present in percentage and number of controls in each column.

Table 1: Capability Maturity Model Integrated (CMMI)

Level	Name	Description
0	Non-existent	Complete lack of any recognizable processes. The enterprise has not even recognized that there is an issue to be addressed.
1	Initial/Ad Hoc	There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
2	Repeatable but Intuitive	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
3	Defined Process	Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.
4	Managed and Measurable	Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5	Optimized	Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Table 2: Number of Controls in Each Category

COBIT Chapter	# of Controls
Plan and Organize (PO)	37
Acquire and Implement (AI)	31
Deliver and Support (DS)	124
Monitor and Evaluate (ME)	14

Table 3: Controls Disposition: Pass, Fail, Partial. First division by type of organization and subdivision by location.

Type	Pass	Partial	Fail
Non Profit	28% (n=21)	19% (n=14)	53% (n=40)
North	18% (n=7)	18% (n=7)	64% (n=25)
South	39% (n=14)	19% (n=7)	42% (n=15)
Private	35% (n=46)	22% (n=29)	43% (n=56)
North	40% (n=36)	24% (n=22)	36% (n=33)
South	25% (n=10)	18% (n=7)	58% (n=23)
Totals	**33% (n=67)**	**21% (n=43)**	**47% (n=96)**

Table 4: Tabulation of results classified by COBIT's domains

PO	24.32% (n=9)	18.92% (n=7)	56.76% (n=21)	37
AI	38.71% (n=12)	22.58% (n=7)	38.71% (n=12)	31
DS	33.87% (n=42)	21.77% (n=27)	44.35% (n=55)	124
ME	28.57% (n=4)	14.29% (n=2)	57.14% (n=8)	14

Table 5: Group Statistics – controls type

Control Type	N	Mean	Std. Deviation	Std. Error of Mean
Managerial Controls	40	.5321	.42367	.06699
Operational (technical) Controls	43	.4956	.40030	.06105

Appendix A

COBIT's Information security controls shown in Table 6 are most important ones used in this research. The table has three columns: a COBIT process identifier consisting of the domain, process number and sub process number. The second column is the title given to the process by COBIT. The third column provides a detailed explanation of the specific sub-process.

Table 6: Select COBIT Controls

PO2.3	Data Classification Scheme	Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.
AI3.1	Technological Infrastructure Acquisition Plan	Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organization's technology direction.
DS4.2	IT Continuity Plans	Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.
DS4.9	Offsite Backup Storage	Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.
DS5.1	Management of IT Security	Manage IT security at the highest appropriate organizational level, so the management of security actions is in line with business requirements.
DS5.2	IT Security Plan	Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.
DS5.3	Identity Management	Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.
DS5.4	User Account Management	Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users,

		including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.
DS5.9	Malicious Software Prevention, Detection and Correction	Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).
DS5.10	Network Security	Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.
DS7.2	Delivery of Training and Education	Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers, and mentors. Appoint trainers and organize timely training sessions. Record registration (including prerequisites), attendance and training session performance evaluations.
DS11.2	Storage and Retention Arrangements	Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organization's security policy and regulatory requirements.
DS11.5	Backup and Restoration	Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.
DS12.2	Physical Security Measures	Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.
DS12.3	Physical Access	Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.