2010

Is it all good? Evidence about IS/IT risks from SEC filings.

Eileen Z. Taylor

Christopher Davis
davisc@mail.usf.edu

Jennifer Blaskovich

Recommended Citation
Taylor, E.Z, Blaskovich, J. & Davis, C.J. (2010). Is it all good? Evidence about IS/IT risks from SEC filings. Presentation at the 2010 Mid-Year Meeting of the Information Systems Section of the American Accounting Association. Clearwater Beach, FL.

IT Risk Disclosure, Governance and Compliance: complementary or conflicting agendas?

Eileen Z. Taylor, Ph.D., CPA*
Department of Accounting
North Carolina State University
919-513-2476
eileen_taylor@ncsu.edu

Jennifer Blaskovich, Ph.D., CPA
Department of Accounting
University of Nebraska – Omaha
402-554-3984

Christopher J. Davis, Ph.D.
College of Business
University of South Florida – St Petersburg
727-873-4944

November 13, 2009

*Corresponding author
Keywords: enterprise risk management, information systems, information technology, 10-K disclosures

IT Risk Disclosure, Governance and Compliance: complementary or conflicting agendas?

Abstract

In 2005, the Securities and Exchange Commission mandated disclosure in an organization's annual report of significant risks that may adversely affect the company. We examine the risk disclosures of the largest 100 U.S. firms over the period 2004-2006 to determine the extent of coverage of IS/IT risks. We find that IS/IT risks represent less than 4% of total risks disclosed and that 40% of companies do not address a single IS/IT risk. An analysis of disclosures by industry suggests evidence of normative or mimetic isomorphism. We conclude that IS/IT risks are underreported or under-analyzed, giving financial statement users a false sense of IS/IT security.

I. Introduction

In 2005, Canada's Hudson Bay Company suffered a $33.3 million loss following the failure of a new computer based inventory system. Ford's abandonment of a purchasing system at a cost of $400 million in 2004 and the cancellation of the $170 million FBI Virtual Case File paperless system in 2003 both highlight the complexity and significance of risk in computer systems development and operation (Charette 2005, Chua 2009) and in Enterprise Resource Planning implementation failures. The consequences that follow poor or missing risk management in information systems projects are universally unprejudiced: they occur in every country; they affect large organizations and small; commercial, non-profit and governmental, and they have little regard for status or reputation.

Individually and collectively these examples highlight the complexity and unpredictability of the risk factors intrinsic to information systems and information technology (IS/IT). The accelerating pace of IS/IT innovation only serves to amplify the potential for failures. The financial services industry highlights this potentiality. The range and sophistication of financial products, services, relationships and regulations have both increased in lock-step with the dynamic, innovative e-commerce systems that support them. An extensive network of complex business processes and interrelationships with regulators, customers, and other institutions characterize contemporary financial services. Any disruption to the IS/IT infrastructure that enables these processes and relationships will reverberate throughout this service chain (Zhu, Kraemer and Dedrick 2004). Although the financial services industry was, and remains, in the forefront of IS/IT innovation, organizations in most other sectors of the economy have adapted or adopted similar capabilities and technologies, creating a web of interconnectivity amongst themselves and their customers. Today IS/IT is fundamental to the exchange of goods, services,

and information in the increasingly diverse global marketplace. IS/IT have become mission critical to many organizations: to that end, the financial services sector provides a useful exemplar of the characteristics of that dependence. As an increasingly wide range of organizations continue to invest time and resources in strategically important IS/IT, managing the risk associated with them becomes a critical area of concern.

The examples above also suggest that IS/IT risks are frequently overlooked, misunderstood or ignored and consequently underappreciated and undervalued (Wallace, Keil and Rai 2004, Kumar 2002, Osmundson, Michael and Machniak 2003). Soberingly, a study by the Project Management Institute shows that risk management is the least practiced of all project management disciplines across all industry sectors, and that nowhere is it less frequently applied than in the IS/IT industry (Charette 2005). Without effective risk management, neither managers responsible for IS/IT development and deployment nor those in business units where the systems are used have any substantial insight into what may go wrong, why it may go wrong, and what they may do to eliminate or mitigate the risks. However, when these risks materialize, the high dependence of business operations on IS/IT often leads to their threatening a wide range of organizational processes, disciplines and divisions. IS/IT have become mission critical to commercial enterprises, as our examples show. Simultaneously, the scope, complexity, and opacity of these risks increases as complex, enterprise-spanning applications are integrated and information systems migrate to more sophisticated technology platforms such as Web2.0 and 'clouds' that are increasingly abstract from the day-to-day experience of workers on the shop floor, trading floor or other physical setting where they are used. As these risks become reality, they result in harm to not only customers, vendors, and creditors; they ultimately injure the equity owners of the business. These rapidly increasing risks and management's difficulty in

identifying and addressing them prompted the Securities and Exchange Commission (SEC) to mandate risk disclosure for all U.S. publicly traded companies in 2005. [1,2]

The primary goal of the SEC is to protect external parties (i.e. the public); one method is to regulate disclosures so that these external parties (e.g. investors, creditors, and vendors) have the information necessary to make informed decisions about doing business with a particular company. Although it provides a comprehensive framework designed to accommodate registrants in all sectors of the economy, Regulation S-K supports a holistic perspective of organizational risk, requiring disclosure of risks that are specific and perhaps unique to the registrant (company) rather than superficial or 'broad brush' analyses that identify only general business or industry risks. Such a holistic perspective of risk and risk management is a key means by which to improve regulatory oversight.

In this exploratory study, we analyze the U.S. Fortune 100 companies' 10-K 1a risk factor disclosures in the years 2004-2006. We propose and answer research questions related to the frequency, proportion, ranking, and change over time of IS/IT risk factor disclosures. We also explore whether there are differences between industries. We use the Trust Services Framework to further analyze the nature of IS/IT risk disclosures, coding them in relation to security, availability, processing integrity, confidentiality, or privacy.

We find that over the three years 2004-2006, IS/IT risks represent less than 4% of the total risks disclosed in the SEC 10-K filings. Approximately 40 percent of the companies in our sample report not a single IS/IT risk. These figures suggest one of two possibilities. Either, despite the frenzied media coverage that follows failures such as those noted earlier, management overlooks, misunderstands, undervalues, or ignores IS/IT risks; or management

[1] The SEC approved Item 503 (c) under Regulation S-K on June 29, 2005. It is effective for issuers with fiscal year ends following December 15, 2005 (Securities and Exchange Commission 2004, 2005).
[2] These companies are also referred to as registrants.

recognizes these risks but does not report them in the 10-K filing. We suggest that the second option is unlikely, given the continued reports of costly system failures. We believe it is more likely that the low disclosure rates are a consequence of a rather superficial appreciation of the reporting and disclosure requirements. Rather than view regulation S-K as an opportunity to embrace risk management as a means to improve corporate performance, management views the disclosures as a compliance issue. By following the letter, rather than the spirit of the regulation, companies themselves and external parties are shortchanged. We explore institutional isomorphism as the theoretic basis for this behavior.

The remainder of the paper falls into six sections. The literature review in Section II elaborates our motivation for this research and explains the development of our research questions: these are set out in Section III. Section IV presents our results. In Section V, we discuss our findings, limitations of our study, and some implications for future research.

II. Literature Review

Although organizations have practiced some form of risk management for decades, the spotlight has intensified in recent years, as stakeholders demand more information about key organizational risks. Since 1997, the SEC has required organizations to disclose quantitative and qualitative information about market risk exposures from financial instruments (Securities and Exchange Commission 1997). However, IS/IT failures such as those discussed by Charette (2005), together with the corporate accounting scandals and business collapses of the early 2000's, clearly showed that organizations face many other types of risks. Thus, the SEC implemented stronger regulations relating to risk disclosure in corporate annual and quarterly reporting. Regulation S-K was intended to alert investors and others to the wide range of risks

involved in owning, loaning to, or doing other business with public companies. The regulation requires that companies list and discuss"…the most significant factors that may adversely affect the issuer's business, operations, industry, or financial position, or its future financial performance" within their 10K filing (Securities and Exchange Commission 2004, 2005) . The SEC identifies three broad categories of risk factors: industry risks (e.g., an inability to acquire raw materials or to meet production demands); company risks (e.g., an inability to acquire software technology or consequences from unionized labor strikes); and investment risks (e.g., inability to pay dividends or a lack of a liquid market for securities) (Securities and Exchange Commission 1999). It is important to note that the SEC included the caveat "where appropriate" in the description guiding risk factor disclosures. Doing so allows management to decide what risk factors it will disclose, and when it will disclose them.

The S-K regulation is relatively new: consequently, little research exists about the types of risks organizations choose to disclose. This paper takes a first step by exploring corporate disclosures regarding IS/IT issues. We focus on these disclosures because information systems underlie virtually every process in business today. The efficiency and effectiveness of internal business operations and compliance with external reporting regulations have long since been dependent upon the IS/IT infrastructure (Rainer, Snyder and Carr 1991). Dependence on increasingly complex technologies has redefined corporate risk, creating the potential for problems that may produce outcomes ranging from inconvenience to catastrophe (Barton, Shenkir and Walker 2002, Loch, Carr and Warkentin 1992, Meall 1989, Stoneburner, Goguen and Ferlinga 2002).

Researchers have long recognized IS/IT as a primary concern in the uncertain and risky business environment. A recent review of the literature cited hundreds of articles, dating back 30

years, that discuss IS/IT risks (Sherer and Alter 2004). Those risks continue to proliferate. The rapid pace of technological advancement, increased interconnectivity, and complex enterprise spanning systems expose organizations to greater risks from business interruption, process interdependency and systems security breaches than ever before (O'Leary 2000, Hunton, Wright and Wright 2004, Cavusoglu, Cavusoglu and Raghunathan 2004).

Earlier regulatory reforms enacted in the wake of Enron and other business failures further increased management's attention to IS/IT risks. Indeed, inadequate systems controls were cited as a chief source of material weaknesses in SEC filings upon the implementation of SOX and the Public Company Accounting Oversight Board requirements (Solomon 2005). Increasing awareness of and sensitivity to the importance of identifying and managing systems risk prompted President Obama to call for the creation of a cyber security czar to protect the nation's digital infrastructure from hackers (Simpson and Cole 2009).

Few businesses are immune to IS/IT risks. Once thought to be the concern of traditionally high-risk industries such as medicine, defense and airlines, IS/IT dependence is now a critical issue for all sectors of the economy (Cavusoglu, Cavusoglu and Raghunathan 2004). Studies place the estimate of companies that have experienced major control failures or systems security breaches at 60% to 80% (e.g., (Cavusoglu, Cavusoglu and Raghunathan 2004, Romney and Steinbart 2009). Increasing speed and decreasing costs explain the ubiquity of IS/IT and, in turn, the accelerated innovation and growth of information-based products and services. Such growth has been particularly significant in the financial services sector (see, for instance Zhu, Kraemer and Dedrick 2004).

Prior research shows that, despite their ubiquity, user communities and management tend to pay less attention to the contribution of IS/IT once they are in operation: IS/IT have become

commoditized and taken for granted (Carr 2003). Consequently, mission criticality often becomes masked by the normal operation of the systems, which themselves become part of the undiscussed social routine of contemporary organizational life. Clearly, businesses are keenly aware of the opportunities presented by the growing reach of 'e-commerce'. It is our contention that the ever-increasing diversity and complexity of intra- and inter-organizational IS/IT systems gives rise to an unrealized degree of dependence on them, and perhaps an underappreciated range of 'e-risks'.

The examples in our introduction show that the tangible and intangible costs of these risks and failures can be high. Tangible costs include items such as lost sales, materials and labor, broken contracts, legal liabilities, and lost market value (Cavusoglu, Cavusoglu and Raghunathan 2004). Loss of consumer confidence, damage to supplier and partner relationships, and exposure of proprietary secrets are difficult if not impossible to quantify. Clearly, this reality makes IS/IT risks a primary concern for accountants, auditors, IT professionals, and managers, whose job it is to manage risk.

Several groups such as the Basel Committee on Banking Supervision have addressed the need for integration of risk factors into comprehensive management strategies that facilitate not only risk identification, but also diagnosis and treatment through the development of risk mitigation, business continuity and disaster recover policies. However, results from a recent survey show that "there is an urgent need to evaluate existing risk management processes in the light of perceived increases in the volume and complexity of risks and 'operational surprises' experienced (Beasley, Branson and Hancock 2009, 20).

Despite Regulation S-K and advice to adopt a more holistic approach to risk oversight, disclosure, and management, Beasley et al. note that "…not all organizations are modifying their

procedures for identifying, assessing, managing and communicating risk information to key stakeholders (op cit, p2). Even though 62% of their respondents indicated that the volume and complexity of risks had changed 'extensively' or 'a great deal' in the last 5 years, "the level of risk management sophistication remains fairly immature for most respondents" (op cit, pp 9 and 19). They go on to report that most organizations appear to lack some of the most fundamental methodologies that would allow them to develop a consistent and reliable view of risk.

The absence of such methodologies or other guidance suggests the existence of a void or discontinuity in the risk management process: this is characterized by the reported unstructured, *ad hoc* communication of risks within organizations. Regulations such as S-K appear directed at this void, providing a means to modify procedures in response to risks that are identified and disclosed. Our research explores the extent to which Regulation S-K has filled the void.

III. Research Questions

IS/IT Risk Disclosure Pervasiveness

Our first set of research questions explores the frequency and proportion of IS/IT risks disclosed in the year prior to the regulation (2004), the year of implementation (2005) and the first full effective year (2006).

RQ1a: What is the frequency of IS/IT risk disclosures?

RQ1b: What proportion of total risk disclosures relate to IS/IT?

Recent studies, particularly one by Beasley et al (2009), suggest that management views risk disclosure primarily in terms of compliance, rather than as an opportunity to institute a holistic risk management process. Our second set of research questions explores the validity and significance of this inference.

If, as the research summarized above suggests, risk disclosure is attenuated by the communication vacuum or void found in many organizations, the effect of regulations such as S-K may not be those intended by their authors, giving rise to a paradox: in the absence of an internally consistent and reliable view of risk, managers in organizations might use the S-K regulation as a surrogate for more comprehensive, locally relevant procedures for identifying risk.

Institutional Theory (DiMaggio and Powell 1983) highlights the paradox faced by regulators. Although clearly a step forward in filling the void and formalizing *ad hoc* communication about risk, regulations such as S-K can have unanticipated consequences in the absence of organizationally specific (and therefore relevant) strategies and processes.

If seen as a time-specific, one-off compliance action, risk disclosures might, over time, homogenize rather than diversify to reflect the growing range of risks intrinsic to IS/IT in business. Such homogeneity arises as institutions, and the people who manage them, seek legitimacy. Clearly, such a quest could be prompted by regulations such as S-K. Homogenization within and between organizations is driven by three pressures: coercion, mimesis, and norms. Coercive pressures result from dependence on other entities such as bureaucratic agencies and powerful constituencies. Organizations gain legitimacy by meeting the directives of these bodies. Mimetic pressures develop when uncertainty in the environment encourages the imitation of practices or actions taken by peer organizations. By mimicking other 'successful' firms, the organization gains a degree of legitimacy. Normative forces result from the desire to conform to norms standardized by professional organizations and corresponding educational requirements. In this case, individuals (i.e., managers) provide a sense of legitimacy by meeting the entrance

requirements of peers within the same profession. Managers become homogenized or interchangeable because of similar backgrounds, experience, and training.

Following Lai et al (2006), we explore changes in IS/IT risk factor disclosures in order to gather evidence about the homogeneity of these corporate disclosures. Based on our knowledge of increasing dependence on and complexity of information systems, and the related risks accompanying those increases, we should observe concomitant increases in IS/IT risk disclosures. Failure to observe these increases supports the institutional isomorphism effect, and thus supports the contention that managers are responding to the regulation with compliance behavior, conforming to the letter, rather than the spirit of the law, and that institutional isomorphism explains this compliance-oriented behavior.

RQ2a: Has the frequency of IS/IT risk disclosures changed over time?

RQ2b: Has the proportion of IS/IT risk disclosures changed over time?

Industry Differences

The variation between industry sectors is the degree to which they depend on IS/IT to support core business processes provides an additional important and orthogonal indicator of the homogeneity discussed above. The substantial prior research on IS/IT investments (including Kohli and Devaraj, 2004; Demirhan et al, 2005; Bhatt and Grover, 2005; Bardhan et al, 2004 and 2006; Zhu, Kraemer and Dedrick, 2004) focuses at the organizational and process levels. Comparison of IT investment between industry sectors is not easy to assess using these measures. We anticipate that companies in highly regulated industries that depend heavily on IS/IT to support their core business processes are likely to report more IS/IT risk factors than companies in less-regulated, less IS/IT dependent industries. For example, we would expect companies in financial services, health care and telecommunications to report more IS/IT risk

factors than companies in manufacturing, tourism and oil and gas. We pose the following questions to explore the differences between the prevalence of IS/IT risk disclosure between industry sectors and their relative significance.

RQ3a: Is there significant variation between industry sectors on the *frequency* of IS/IT risks disclosed?

RQ3b: Does the *relative significance* of IS/IT risks disclosures vary between industry sectors?

Trust Services Framework

After exploring the frequency, proportion, and changes over time related to IS/IT risk factor disclosures we conduct additional analyses on those disclosures to understand the types of risks actually reported. Wallace et al. (2004) highlights the paucity of suitable categorical schemes to support the classification of IS/IT risks. Although a range of checklists and other frameworks have been proposed "…there are relatively few tools available to help project managers identify and categorize risk factors in order to develop effective strategies" (Wallace, Keil and Rai 2004, 115). Recently, comprehensive governance frameworks such as CobiT (Control Objectives for Information Related Technology) have emerged to supplement predecessors such as COSO (the Treadway Commission's Committee of Sponsoring Organizations). CobiT has become widely used to assess the internal controls and overall corporate governance of an institution (Tuttle and Vandervelde, 2007). One of the 34 high-level CobiT processes addresses the assessment and management of IT risk. However, although CobiT has 215 specific and detailed control objectives throughout these 34 high-level IT processes, its evolution as a governance mechanism did not lend itself to our classificatory objectives.

The more recent Trust Services Framework, developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), is a set of core principles and criteria that directly address the reliability of a company's information technology and systems (AICPA and CICA 2006). In addition to providing a robust and well-known typology of risk categories, the Trust Services Framework provides a means to accommodate and categorize risk disclosures from all sectors of the economy, not just banking and financial services. The framework identifies five fundamental principles that focus on individual aspects of systems controls and governance. Security, the first principle, forms the foundation of the framework and supports the other four principles (Romney and Steinbart 2009). It addresses controls and policies that are designed to protect the IS/IT operations and development processes from unauthorized access. The remaining four principles are availability, processing integrity, confidentiality, and privacy. Availability refers to the accessibility of the system for processing, monitoring, and maintenance. Processing integrity addresses the completeness, accuracy, and timeliness of system processing. Confidentiality refers to the protection of organizational information designated as confidential (e.g. business plans, customer lists, internal pricing). Finally, privacy focuses on the protection of information an organization holds regarding its customers, suppliers, and employees. Together, the five principles contribute to the ultimate goal of achieving systems integrity and minimizing systems risk exposures (AICPA and CICA 2006).

The Trust Services principles were developed to attune organizations to the risks posed by their IS/IT environment (AICPA and CICA 2006). The increasing dependence on IS/IT in every aspect of an entity's operations is matched only by the increasing concern over the systems' reliability. All variety of stakeholders, including boards of directors, creditors, regulators,

business partners, and customers, rely on IS/IT for timely and relevant information. Yet, reliability remains a question for even the best-designed systems. The CICA (Canadian Institute of Chartered Accountants 2009) notes that the complexity of todays IS/IT systems make them "breeding grounds for errors and other compromises to data" (p1). Furthermore, because the systems are interconnected, errors in one entity's system travel downstream, well beyond the boundaries of the entity (Canadian Institute of Chartered Accountants 2009). The Trust Services Framework provides professional guidance for identifying and addressing these risks (Coe 2005).

We use this framework to classify the data, deepening our understanding of the distribution of disclosed risks among the five principles. (Examples of risk disclosures categorized by Trust Services principles are provided in Appendix B). It is important to recognize the fundamental characteristic of the Framework that all five principles must be addressed in order to ensure systems reliability. Because most experts agree that it is impossible to eliminate the risks addressed in the Trust Services Framework entirely (Romney and Steinbart 2009), we might expect that entities would recognize risks pertaining to each area. Our final research questions examine this expectation and explore whether this distribution has changed since the regulation was enacted. We look for evidence of changes in the distribution to determine if companies are addressing more (or less) of the IS/IT risk spectrum as the regulation matures. With a view to understanding the motivation guiding these disclosures, we ask:

RQ4a: What is the distribution of IS/IT risk factor disclosures among the five Trust Services principles?

RQ4b: Has the distribution of IS/IT risk factor disclosures among the five Trust Services principles changed over time?

IV. Results

We select our sample by identifying the Fortune 100 companies (based on total sales) for the year 2004 (see listing in Appendix A). We limit our analysis to these companies for three reasons. First, these companies likely have the resources and competency required to engage in enterprise risk management, second, they are more likely to be under the SEC's watchful eye, increasing extent of compliance likelihood, and third, other firms are likely to view their actions as setting a standard or norm for reporting decisions. We eliminate five mutual insurance companies that are not publicly traded, leaving an initial sample of 95 firms. In order to appropriately address our research questions, we then follow these 95 firms over the three year period, 2004-2006. We believe this method best allows us to analyze the changes in risk factor disclosures over the three-year period surrounding the mandate. During this period, four of the firms merged into one firm, further reducing the sample. Three of the firms merged in 2005, with the fourth merging in 2006. Thus, our sample of 95 firms in 2004 (the year prior to the introduction of Regulation S-K) is reduced to 93 firms in 2005 and 92 firms in 2006 (the first full year of operation).

We downloaded the company name, industry code, total average assets, total average sales, and Fortune rank from the Compustat database. Then we located and hand-collected the text and rank from each Item 1a of each company's 10-K for the related year.[3] We built a relational database to store all data. Two graduate assistants independently coded the data as follows:

1 – Indicate whether each risk factor was IS/IT related.

2 - If a factor was IS/IT related, code it as related to one or more of the Trust Services Principles (based on a short description provided).

[3] Rank indicates the sequential order in which risk factors appeared. While companies do not generally number factors, they often appear in a list format.

Inter-rater agreement was 97.2% on whether each risk factor was IS/IT related. Within the set of IS/IT risk factors identified by both raters, inter-rater agreement on coding of the risk factors into the Trust Services Principles was 87.3%. Inter-rater reliability was found to be Kappa = 0.941, which represents a very high level of agreement (Landis and Koch 1977). Differences were resolved through review and discussion between one of the researchers and an independent party who teaches Accounting Information Systems courses at a large university.

We examined 280 10-K reports, resulting in the collection of 3,795 individual risk factors from the three-year period: 2004, 2005, and 2006. Participation in 2004 was lowest, with only 65 companies reporting risk factors. By 2005 and through 2006, all companies in our sample reported at least one risk factor. The average number of risk factors per company per year increased slightly, from 13.28 in 2004 to 16.27 in 2006, as did the maximum number of risks per company, from 41 to 48. The distribution of risk factors over the three years appears in Table 1 below.

==========Table 1 about here ==========

The frequency distribution of all risk disclosures during this period reflects the upward trend in Table 1. However, it is interesting to note the modest increase in the number of registrants reporting higher numbers of risk factors (Figure 1).

========== Figure 1 about here ==========

Turning to the data specific to IS/IT risk disclosures that address research question 1a, we find that the prevalence of IS/IT risk disclosures is relatively low – with 18 companies reporting at least one IS/IT risk factor in 2004, 47 in 2005, and 55 companies reporting at least one IS/IT risk factor in 2006 (see Table 2). Table 2, Panel A summarizes data that respond to research question 2a, regarding the change in frequency over time. Over the period 2004-2006, we note a

steady increase in both the total number of risk factors reported, as well as an increase in the total number of companies reporting at least one IS/IT risk factor, as noted earlier. In 2004, the year before the mandate, only 18.9 percent of Fortune 100 regulation S-K eligible companies reported at least one IS/IT risk factor. That percentage increased to 50.5 percent in 2005, and 59.8 percent in 2006. Nevertheless, the absence of any IS/IT risk factor disclosure from over 40 percent of the largest companies filing under regulation S-K is surprising.

We explored this issue more deeply: the data that address research questions 1b and 2b - the percentage of IS/IT-related disclosures to all risk disclosures are summarized in Table 2, Panel B. The data reveal that although risk disclosures overall are increasing, those related to IS/IT represent a relatively small portion (3.7 percent of all risks disclosed over the three year period). This proportion has increased slightly over time - from 2.1 percent of the total risk factors disclosed in 2004 to 3.3 percent in 2005 and 3.7 percent in 2006. Although the proportion of IS/IT risk factor disclosures has increased, this increase is from a very low initial threshold and does not appear to reflect the large increase in IS/IT risks we observe in practice.

We also note that IS/IT risks consistently appear later in disclosures than non-IS/IT risks, measured as the average location of IS/IT risk factors, compared with the average location of non-IS/IT risk factors (Table 2, Panel B). The overall average rank of non-IS/IT risks factors is 10.5, while the overall average rank for IS/IT risk factors is 13.0. While rank is not necessarily indicative of risk importance, absent objective processes for risk ranking (e.g. alphabetical, functional area), rank is decided by someone at some time, and thus provides information about management's choices.

==========Table 2 about here ==========

Next, we evaluate the data at the industry level to answer research questions 3a and 3b, regarding industry differences in the frequency and proportion of IS/IT risks disclosed. Table 3 lists the specific industries that had at least one company report IS/IT risks as at least 10 percent of their total risks reported (2004-2006). Of the 56 industries represented in the Fortune 100, six qualified. Presented in Table 3, these industries in descending order (percentage of total risk factors that are IS/IT-related) represent Finance and Radio, TV, and electrical stores (25 percent), department stores (13.3 percent), hospital and medical service plans (12.4 percent), general medical and surgical hospitals (11 percent), and plastics (11 percent). It is not surprising that department stores, which are heavily dependent on IS/IT for revenue generation, purchasing, record keeping, and distribution, recognize more IS/IT risks. Likewise, financial services and hospitals, whose operations heavily depend on IS/IT, are also closely regulated, making disclosure even more likely. What is disconcerting is that 50 industries out of 56 (89 percent) list fewer than 10% of their risks as IS/IT-related. These industries include telecommunications, insurance, oil and gas, pharmaceuticals, and computers (including software). While we acknowledge that companies in these industries may be able to mitigate some risks through avoidance or sharing, it is likely that some IS/IT risks remain. Further, a review of the data finds that 27 industries (48 percent) had no companies list even one IS/IT risk. These industries (total risk factors listed for 2004-2006) include computer programming and data processing (106), public warehousing (86), guided missiles and space vehicles (51), television broadcasting (50), and meatpacking (43).

========== Table 3 about here ==========

The summary data in Table 4 shows variation between industry groupings and provides additional insight into industry differences. The data represents average risk rank for IS/IT risks

disclosed in the S-K filings. The data have been sorted: lower values (towards the top of the table) indicate that those risks are ranked earlier in the risk disclosure. For example, computer and software wholesalers list IS/IT risks earlier in the disclosure, while computer communication equipment retailers list those risks later. In response to research question 3b, it appears as though the relative significance of risk disclosures varies between industry sectors, however, we discern no predictable pattern.

========== Table 4 about here ==========

Our final analysis relates to the nature of IS/IT disclosures, research questions 4a and 4b, using coding based on the Trust Services Framework. It should be noted that an individual risk factor could relate to more than one principle (e.g. the risk of system failure could relate to processing integrity and availability).

In response to research question 4a, the distribution among the five Trust Services principles is weighted toward risks that threaten system availability (69 risks, 57.5 percent of all IS/IT related risks). Following availability, security threats are mentioned 61 times (50.8 percent), with processing integrity threats not far behind, with 60 (50 percent). Threats to confidentiality, 22 (18.3 percent) and privacy, 20 (16.7 percent) are the least frequently mentioned. We summarize these findings in Table 5.

========== Table 5 about here ==========

Companies may report availability threats most frequently because IS/IT availability is a necessary component to system function. Since many business processes rely on IS/IT, if those systems are down, none of the processes may proceed. In IS/IT-dependent businesses, unavailable systems prevent revenue from being earned and/or collected, payroll from being processed, bills from being paid, and a host of other activities from continuing. Compared with

the other threats, system availability is clearly the most significant. However, despite the clear prevalence of these risks in our analysis, we believe that they are still significantly under-represented. Two factors prompt this observation. Firstly, our findings in response to RQ2b, rate of change over time, suggest substantial under-reporting of these risks. Secondly, we find it difficult to comprehend how managers within industries that are ostensibly 'risk free' according to their disclosures - computer programming and data processing, guided missiles, and meatpacking - are unaware of their businesses critical dependence on high integrity IS/IT. This suggests that the risks themselves have been insufficiently analyzed in-house and are therefore under-appreciated, exacerbating the low rate of reporting. This concurs with Benaroch et al (2006) who found that managers in a financial services setting relied on intuition to assess IT investment risk rather than any formal method or framework.

Processing integrity threats and security threats each represent about one-half of total IS/IT threats reported. Both may result in errors in business processes or accounting, leading to losses related to inaccurate data, loss of customer confidence, and expenditures to correct errors.

Companies report risks associated with confidentiality and privacy least frequently. There are several potential explanations for this finding. First, companies may not recognize these threats as serious, second, they may have taken measures to mitigate these risks, and third, they may not want the public to know that these threats exist.[4] Figure 2 presents risk factors by principle as a percentage of total IS/IT risk factors over time. In response to research question 4b, changes in distribution over time, we observe that confidentiality and privacy are increasing as a percentage of total IS/IT risk factors over the three-year period.[5] This may indicate an increase in

[4] We acknowledge that these risks may be singular, and therefore companies may adequately discuss them in a single disclosure, however, one could say the same for other types of risks.

[5] None of the major privacy regulations were enacted during the time period we examined. The Financial Modernization Act was implemented in 1999 and the Health Insurance Portability and Accountability Act was first

corporate awareness of these two types of IS/IT risks, however, the data show that reporting of availability and processing integrity risks is declining, perhaps suggesting some sort of trade-off of risk awareness.

========== Figure 2 about here ==========

Post-Hoc Analysis: Financial Characteristics

We also considered whether there were differences in certain financial characteristics of IS/IT risk reporting versus non-reporting companies. While we acknowledge there is little financial variation in the Fortune 100 companies, we explore the possibility of uncovering significant differences in total assets and/or total sales. Statistical analysis (non-tabulated) reveals that neither total assets nor total sales are statistically significantly different between reporters of IS/IT risks and non-reporters.

V. Discussion, Future Research, and Limitations

We find that IS/IT risks are generally under-analyzed (or underreported) by organizations, giving investors; creditors; customers and the public at large a rather naïve (and false) sense of security. Although our modest sample size makes generalizations rather speculative, we are surprised by the low rates of IS/IT risks presented by the top US companies. Indeed, close to half of the Fortune 100 companies do not acknowledge any risk exposure related to their own critical infrastructure.

Although an important addition to the regulatory process and an alternative lens through which to maintain oversight, the S-K regulation limits itself. It is a uniform medium: this is both a strength and a weakness. The strength of regulatory uniformity arises from codification,

enacted in 1996 and revised in 2003. The Family Educational Rights and Privacy Act was finalized in 2008. This act protects the privacy of student educational records, and does not affect the companies in our sample.

methodization, and systematization – the presentation of order. The weakness is the tendency for users of the regulation to *conform* rather than *inform* – that is to say, to comply with the minutiae of the regulation, rather than use the regulatory framework as a guide to investigate, explore and expand the representation to accommodate known and emerging risks.

In order for companies to comply with regulation S-K, it is essential that they develop a comprehensive, organizationally relevant risk management strategy. Without such a strategy, it is impossible to effectively identify and manage their IS/IT in ways that fully meet the S-K mandate.

The failure to comprehensively integrate risk factors into management strategy and thereby support a truly effective governance mechanism prompts Linsley and Shrives (2006) to suggest that risk disclosures are regarded a function of conformation rather than compliance: that organizations "…may just be conforming to a quasi-norm whereby larger companies believe they should disclose more information, risk or non-risk". Their observations resonate with our characterization of Regulation S-K and other instruments being adrift in a strategy void or vacuum. The uniformity and codification of S-K and other regulatory instruments become an ends rather than a means to an end. In this situation, regulatory instruments act like cages rather than frameworks.

Haunschild and Miner (1997) suggest that in situations of uncertainty, social factors substitute for technical criteria and imitation takes the place of investigation and independent choice . While companies may be able to identify and quantify some risks, uncertainty about limitless other potential occurrences remains. Companies may respond to this uncertainty through the mechanisms of institutional isomorphism. In striving to conform and comply, organizations seek legitimacy; coercive, mimetic, and normative pressures affect the

interpretations and behaviors of those charged with disclosure. Most significantly, in our view, coercive pressure may encourage compliance with the letter of the law rather than the spirit of the law. Rather than use the disclosure mandate as an opportunity to inform themselves about the efficacy of their organization's risk management strategy and processes, and investors and others of the risks acing the organization, registrants appear to have taken a compliance approach In sum, management discloses risk factors because the SEC mandates they must disclose risk factors, not because they aim to inform investors, or even improve their own management approach.

Our findings related to industry difference indicate the influence of mimetic and normative pressures. The data are more homogenous than we would anticipate for such a diverse range of industries: the absence of any IS/IT risk disclosure in some industries may be the result of organizations mimicking the disclosure practices of others. In uncertain environments, organizations will mimic other organizations because they perceive safety in numbers. This makes intuitive sense: if an organization discloses a risk that a main competitor does not, does the disclosing organization become more risky in the eyes of the investor? By mimicking the practices of intra-industry peers, an organization can avoid this perception. The homogeneity in our data may also be explained by normative isomorphism, which predicts that managers within similar professions develop similar perceptions or frames of reference: managers within an industry are likely to have the same background and experiences, consequently their decisions on disclosure may become consistent.

We also find an increase in confidentiality and privacy-related risk disclosures, at a cost to availability and processing integrity disclosures. This shift may represent a response to media reports and regulatory pressures regarding identity theft and corporate espionage. However,

mimetic pressures may also be a cause of this increase – resulting in generalized disclosures that do little to help investors understand the unique risks facing a particular company.

Our use of institutional isomorphism to explain some of our findings is rather speculative: further investigation is warranted. However, it is clear from the disclosure practices we report that the effectiveness of the S-K regulation is open to question. The objective of the regulation is to provide information to investors and other external parties regarding the risk exposure of an organization. Our results cast doubt on whether organizations are truly informing - identifying risks, exploring their causes and effects, putting in pace processes and strategies to mitigate them and advising regulators and investors of their actions; or are merely conforming - disclosing the minimum required to comply with regulation S-K. Greater transparency in the regulatory process, as proposed by Simpson and Cole (2009), may address this issue, making organizations more accountable internally, and promoting more comprehensive and open reporting that, in turn, will benefit both shareholders and regulators.

In addition to highlighting the challenges that face the writers and users of regulations, this paper makes important initial contributions to our understanding of the managerial and regulatory challenges that surround the use of large-scale integrated IS/IT in corporate America. We demonstrate that the Trust Services framework provides a robust means of classifying IS/IT risk factors that can be used to differentiate their incidence and significance. The initial use of this approach in this paper suggests that it could be used in future research to explore the differences between industry sectors (alluded to in Table 4) and organizations within sectors (Table 3) in order to more fully understand the range, nature and significance of the risks posed by IS/IT systems.

Further research is warranted to examine whether isomorphic forces have resulted in the homogenization of firms' risk disclosures. Are disclosures boilerplate, or do they truly identify risk factors unique to the particular firm? Boilerplate disclosures do not provide the most relevant or valuable information for the investor: failure to optimally use the S-K regulation to guide investigation, exploration and disclosure about IS/IT risks contributes to information overload, masking the potential of the disclosure process to guide management strategy and action. Experimental research offers a suitable methodology for examining the informational effect of the risk disclosures on both management decision making and investor decisions. Investigation of how firms make their disclosure choices and who is responsible for making them can also help us understand the potential motivations or incentives for the disclosures.

Finally, this paper contributes to the scant body of research on risk factors, and particularly, on risk factor disclosure. A handful of studies have investigated general risk-related disclosures in U.K. and Canadian public companies (Linsley and Shrives 2006, Linsley, Shrives and Crumpton 2006) and value-at-risk disclosures in U.S. commercial banks (Jorion 2002). Dobler (2008) reviews discretionary disclosure and cheap talk models to analytically discuss risk reporting incentives. To the best of our knowledge, however, no other published paper has examined the risk factor disclosure regulation. Our paper is a first attempt to address this gap.

We are unable to conclude definitively why the majority of organizations in our sample do not disclose any IS/IT risks. The question remains whether companies do not recognize the risk, whether they recognize but do not disclose the risk, or whether they mitigated the risk such that no disclosure was necessary. Each of these possibilities represents challenges and potential problems for the organization and its stakeholders. If companies do not recognize risks, the potential for catastrophic effects is unchecked. If they recognize but do not disclose, the

regulation has failed to achieve its goal and investors are unaware of a potentially serious exposure. Lastly, companies that feel no need to disclose because the IS/IT risk has been mitigated must be viewed skeptically. As most IS/IT experts agree, it is inherently impossible to fully remove risk from IS/IT systems because of the speed of technology innovation. Future research, particularly surveys or field experiments, offers an avenue to find answers to these questions.

Limitations

The availability and reliability of data relating to Fortune 100 companies provides us with a robust dataset with which to explore our research questions. However, three factors limit this advantage. Firstly, we restrict our sample size to the 100 largest U.S. public companies. While this sample spans a wide variety of industries, it is not inclusive of all industries. Additionally, we cannot generalize results to small or mid-sized companies. Secondly, the SEC's risk factor disclosure regulation is relatively new. Over time, companies may dramatically change the number and/or level of detail in their disclosures. While we have presented three years worth of data, future research should continue to observe and analyze this data, providing a longitudinal perspective. Finally, by restricting our analysis to IS/IT risks, we cannot comment on the appropriateness of corporate risk disclosure in other areas (e.g., financial, environmental, marketing). However, because IS/IT is a rapidly changing field, both with respect to innovation and diffusion; companies are continuously encountering new related risks, and we would have expected companies to include these risks in their public disclosures.

References

AICPA and CICA. *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy.* American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants, 2006.

Barton, T.L., W.G. Shenkir, and and P.L. Walker. *Making Enterprise Risk Management Pay Off.* Upper Saddle River, NJ: Prentice Hall, 2002.

Beasley, M., B. Branson, and B. Hancock. *Report on the Current State of Enterprise Risk Oversight.* Raleigh, NC: ERM Initiative at North Carolina State University, 2009.

Canadian Institute of Chartered Accountants. "Overview of Trust Services." *Canadian Institute of Chartered Accountants.* 2009. http://www.webtrust. org/overview-of-trust-services.

Carr, N. "IT Doesn't Matter." *Harvard Business Review* May (2003): 41-49.

Cavusoglu, H., H. Cavusoglu, and and S. Raghunathan. "Economics of IT security management: Four improvements to current security practices." *Communications of the AIS* 14 (2004): 65-75.

Charette, Robert N. "Why Software Fails." *IEEE Spectrum* 42, no. 9 (2005): 42-49.

Chua, Alton Y.K. "Exhuming IT projects from their graves: An analysis of eight failure cases and their risk factors." *Journal of Computer Information Systems*, Spring 2009: 31-39.

Coe, M.J. "Trust services: A better way to evaluate I.T. controls." *Journal of Accountancy*, March 2005.

Committee of Sponsoring Organizations. *Enterprise Risk Management - Integrated Framework.* New York: COSO, 2004.

DiMaggio, P., and W. Powell. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48, no. April (1983): 147-160.

Dobler, M. "Incentives for risk reporting - A discretionary disclosure and cheap talk approach." *The International Journal of Accounting* 43 (2008): 184-206.

Haunschild, Pamela R., and Anne S. Miner. "Modes of interorganizational imitation:The effects of outcome salience and uncertainty." *Administrative Science Quarterly* 42, no. 3 (September 1997): 472-500.

Hunton, J., A. Wright, and and S. Wright. "Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?" *Journal of Information Systems* 18, no. 2 (Fall 2004): 7-28.

IOMA. "Top priority for new rules targeting financial reporting fraud." *Financial Analysis, Planning, and Reporting* 4, no. 10 (October 2004): 5-6.

Jorion, P. "How informative are value-at-risk disclosures?" *The Accounting Review* 77, no. 4 (Oct 2002): 911-931.

Krebs, Brian. "Obama: Cybersecurity is a national security priority." *The Washington Post*, May 29, 2009.

Kumar, R. "Managing Risks in IT Projects: an options perspective." *Information & Management*, 2002: 63-74.

Lai, K., C. Wong, and T. Cheng. "Institutional Isomorphism and the adoption of information technology for supply chain management." (Computers in Industry) 57 (2006): 93-98.
Landis, J.R., and G.G. Koch. "The measurement of observer agreement for categorical data." *Biometrics* 33 (1977): 159-174.
Linsley, P.M., P.J. Shrives, and and M. Crumpton. "Risk disclosure: An exploratory study of UK and Canadian banks." *Journal of Banking Regulation* 7, no. 3/4 (2006): 268-282.
Linsley, Phillip M., and Philip J. Shrives. "Risk reporting: A study of risk disclosures in the annual reports of UK companies." *The British Accounting Review* 38, no. 4 (2006): 387-404.
Loch, K., H. Carr, and and M. Warkentin. "Threats to information systems: Today's reality, yesterday's understanding." *MIS Quarterly* 16, no. 2 (1992): 173-186.
Meall, L. "Survival of the fittest." *Accountancy*, March 1989: 140-141.
O'Leary, D. *Enterprise Resource Planning Systems: Systems, Life Cycle, Electronic Commerce, and Risk.* Cambridge, MA: Cambridge University Press, 2000.
Oppenheimer, Wolff, and Donnelly, LLP. "SEC Alert 12/1/05: Required new risk factor disclosure in form 10-Ks and 10-Qs." 2005.
Osmundson, J. S., J. B. Michael, and M. J. Machniak. "Quality management metrics for software development." *Information & Management* 40, no. 8 (2003): 799-812.
Pressman, R. *Software Engineering (5th Edition).* New York: McGraw-Hill, 2001.
Project Management Institute. *Innovations: Project Management Research 2004.* Project Management Institute, 2005.
Rainer, Jr., R.K., C.A. Snyder, and and H.H. Carr. "Risk analysis for information technology." *Journal of Management Information Systems* 8, no. 1 (1991): 129-147.
Romney, M.B., and and P.J. Steinbart. *Accounting Information Systems.* 11th edition. Upper Saddle River, NJ: Pearson Education Inc, 2009.
Securities and Exchange Commission. *Division of Corporate Finance: Updated staff legal bulletin No.7 - Plain English Disclosure.* New York: Securities and Exchange Commission, 1999.
—. "Financial Reporting Release No. 48." 1997.
Securities and Exchange Commission. "Release No. 33-8501." 2004.
Securities and Exchange Commission. "Release No. 33-8591." 2005.
Sherer, S.A., and and S. Alter. "Information systems risks and risk factors: Are they mostly about information systems?" *Communications of the Association for Information Systems* 14 (2004): 29-64.
Simpson, Cam, and August Cole. "Obama Moves to Curb Data-System Attacks." *Wall Street Journal*, May 30, 2009.
Solomon, D. "Accounting rule exposes problems but draws complaints about costs." *Wall Street Journal*, 2005: A1, A12.
Stoneburner, G., A. Goguen, and A. Ferlinga. *Special Publication 800-30-a Risk Management Guide for Information Technology Systems.* National Institutes for Standards and Technology, 2002.

Wallace, L., M. Keil, and A. Rai. "Understanding Software project Risk: a cluster analysis." *Information & Management* 42 (2004): 115-125.
Zhu, K., K.L. Kraemer, and J. Dedrick. "Information Technology Payoff in E_Business Environments: An International Perspective on Value Creation in the Financial Services Industry." *Journal of Management Information Systems* 21, no. 1 (2004): 17-54.

APPENDIX A
Listing of Sample Companies – 2005 Fortune 100 (based on 2004 reports)

1	Walmart	34	Dow Chemical	67	Sprint
2	Exxon	35	Albertson's (sold to Supervalu on June 2, 2006)	68	New York Life Insurance
3	General Motors	36	Morgan Stanley	69	Viacom
4	Ford	37	MetLife	70	International Paper
5	GE	38	Walgreen	71	Johnson Controls
6	Chevron	39	United Technologies	72	Tyson Foods
7	ConocoPhillips	40	United Health Group	73	Caremark
8	Citigroup	41	Microsoft	74	JC Penney
9	AIG	42	United Parcel Service	75	Honeywell
10	Intl. Business Machines	43	Lowe's	76	Ingram Micro
11	Hewlett-Packard	44	Archer Daniels Midland	77	Best Buy
12	Berkshire Hathaway	45	Sears Roebuck	78	FedEx
13	Home Depot	46	Safeway	79	Alcoa
14	Verizon	47	Lockheed Martin	80	HCA
15	McKesson	48	Medco Health Solutions	81	TIAA-CREF
16	Cardinal Health	49	Motorola	82	Sunoco
17	Altria	50	Intel	83	Mass Mutual Life
18	Bank of America	51	Allstate	84	Merck
19	State Farm Insurance	52	Wells Fargo	85	St. Paul Travelers
20	JP Morgan Chase	53	Merrill Lynch	86	Duke Energy
21	Kroger	54	Walt Disney	87	BellSouth
22	Valero Energy	55	CVS	88	Hartford Financial
23	AmerisourceBergen	56	AT&T (merged with #33 SBC to form AT&T Inc)	89	Weyerhaeuser
24	Pfizer	57	Caterpillar	90	MCI (merged with Verizon, last filing 12/29/04)
25	Boeing	58	Northrop Grumman	91	Cisco
26	Procter & Gamble	59	Goldman Sachs	92	Coca-Cola
27	Target	60	Sysco	93	Bristol-Myers Squibb
28	Dell	61	PepsiCo	94	Lehman Brothers
29	Costco Wholesale	62	American Express	95	Electronic Data Systems
30	Johnson & Johnson	63	Delphi	96	Plains All American Pipeline
31	Marathon Oil	64	Prudential Financial	97	Wellpoint
32	Time Warner	65	Wachovia	98	News Corp
33	SBC Communications (Merged with AT&T in 11/05)	66	DuPont	99	Nationwide Insurance
				100	Abbott Laboratories

Dropped from original sample (insurance companies)
Merged or failed in 2005
Merged in 2006

Appendix B
Examples of Risk Disclosures categorized by Trust Services Principles

Principle	Risk Disclosure Example
Security	If we are unable to protect our information systems against data corruption, cyber-based attacks or network security breaches, our operations could be disrupted. We are increasingly dependent on information technology networks and systems, including the Internet, to process, transmit and store electronic information. In particular, we depend on our information technology infrastructure for digital marketing activities and electronic communications among our locations around the world and between Company personnel and our bottlers, other customers and suppliers. Security breaches of this infrastructure can create system disruptions, shutdowns or unauthorized disclosure of confidential information. If we are unable to prevent such breaches, our operations could be disrupted or we may suffer financial damage or loss because of lost or misappropriated information.
Availability	Infrastructure failures could harm our business. We depend on our information technology and manufacturing infrastructure to achieve our business objectives. If a problem, such as a computer virus, intentional disruption by a third party, natural disaster, manufacturing failure, or telephone system failure impairs our infrastructure, we may be unable to book or process orders, manufacture, and ship in a timely manner or otherwise carry on our business. An infrastructure disruption could cause us to lose customers and revenue and could require us to incur significant expense to eliminate these problems and address related security concerns. The harm to our business could be even greater if it occurs during a period of disproportionately heavy demand.
Processing integrity	We outsource and obtain certain information technology systems or other services from independent third parties, and also delegate selected functions to independent practice associations and specialty service providers; portions of our operations are subject to their performance. Although we take steps to monitor and regulate the performance of independent third parties who provide services to us or to whom we delegate selected functions, these arrangements may make our operations vulnerable if those third parties fail to satisfy their obligations to us, whether because of our failure to adequately monitor and regulate their performance, or changes in their own financial condition or other matters outside our control. In recent years, certain third parties to whom we delegated selected functions, such as independent practice associations and specialty services providers, have experienced financial difficulties, including bankruptcy, which may subject us to increased costs and potential network disruptions, and in some cases cause us to incur

	duplicative claims expense. Certain legislative authorities have in recent periods also discussed or proposed legislation that would restrict outsourcing and, if enacted, could materially increase our costs. We also could become overly dependent on key vendors, which could cause us to lose core competencies if not properly monitored.
Confidentiality	The success of our business depends on maintaining a well-secured pharmacy operation and technology infrastructure. We are dependent on our infrastructure, including our information systems, for many aspects of our business operations. A fundamental requirement for our business is the secure storage and transmission of personal health information and other confidential data. Our business and operations may be harmed if we do not maintain our business processes and information systems, and the integrity of our confidential information. Although we have developed systems and processes that are designed to protect information against security breaches, failure to protect such information or mitigate any such breaches may adversely affect our operations. Malfunctions in our business processes, breaches of our information systems or the failure to maintain effective and up-to-date information systems could disrupt our business operations, result in customer and member disputes, damage our reputation, expose us to risk of loss or litigation, result in regulatory violations, increase administrative expenses or lead to other adverse consequences.
Privacy	An increase in account data breaches and fraudulent activity using our cards could lead to reputational damage to our brand and could reduce the use and acceptance of our charge and credit cards. We and other third parties store Cardmember account information in connection with our charge and credit cards. Criminals are using increasingly sophisticated methods to capture various types of information relating to Cardmembers' accounts, including Membership Rewards accounts, to engage in illegal activities such as fraud and identity theft. As outsourcing and specialization become a more acceptable way of doing business in the payments industry, there are more third parties involved in processing transactions using our cards. If data breaches or fraud levels involving our cards were to rise, it could lead to regulatory intervention (such as mandatory card reissuance) and reputational and financial damage to our brand, which could reduce the use and acceptance of our cards, and have a material adverse impact on our business.

Figures and tables for inclusion in the body of the manuscript

Table 1
Total Risk Factors by Year

	Number of risk factors	Number of companies reporting at least one risk factor	Mean number of risks per company	Standard Deviation	Range
2004	863	65	13.28	8.67	1-41
2005	1435	93	15.43	8.23	1-42
2006	1497	92	16.27	8.55	1-48

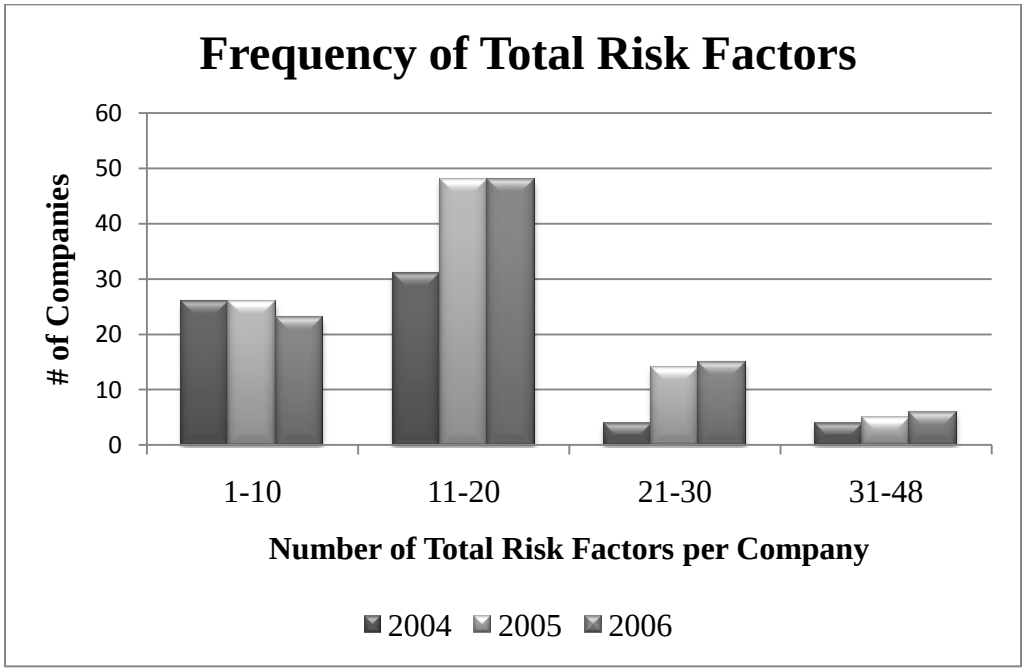

Figure 1

Table 2
Prevalence of IS/IT Risk Disclosures

Panel A

Year	Number of companies reporting at least one IS/IT risk	Total Number of Companies	Percentage of companies reporting at least one IS/IT risk
2004	18	95	18.9%
2005	47	93	50.5%
2006	55	92	59.8%

Panel B

	Year	Number of individual risks	Percentage of total risks	Average rank [a]
IS/IT Risks	2004	18	2.1	14.4
Non-IS/IT Risks	2004	845	97.9	10.0
Total	2004	863	100	
IS/IT Risks	2005	47	3.3	12.4
Non-IS/IT Risks	2005	1388	96.7	10.4
Total	2005	1435	100	
IS/IT Risks	2006	55	3.7	13.1
Non-IS/IT Risks	2006	1442	96.3	10.9
Total	2006	1497	100	
IS/IT Risks	Total	120	3.2	13.0
Non-IS/IT Risks	Total	3675	96.8	10.5
Total	Total	3795	100	

[a] Calculated by sequentially numbering each risk in the company's disclosure. Lower numbers indicate higher ranking.

Table 3
Specific Industries with Companies Disclosing IS/IT Risks Greater than 10% of Total Risks
Total of 2004, 2005, and 2006

Industry	IS/IT risks (a)	Non-IS/IT risks (b)	Total risks (c)	Percentage of total risks that are IS/IT (a/c)
FINANCE-SERVICES	12	36	48	25.0%
RADIO,TV,CONS ELECTR STORES	6	18	24	25.0%
DEPARTMENT STORES	2	13	15	13.3%
HOSPITAL & MEDICAL SVC PLANS	11	78	89	12.4%
GEN MED & SURGICAL HOSPITALS	6	48	54	11.1%
PLASTIC MATL,SYNTHETIC RESIN	2	17	19	10.5%

Table 4
Average Risk Rank for Disclosed IS/IT Risks,
by General Industry Groupings (NAICS)

NAICS	Industry Description	Average IS/IT Risk Rank
423430	COMPUTERS & SOFTWARE-WHSL	4.33
523110	COMMERCIAL BANKS	4.50
334111	ELECTRONIC COMPUTERS	5.33
336322	MOTOR VEHICLE PART,ACCESSORY	6.00
517110	PHONE COMM EX RADIOTELEPHONE	6.00
522291	FINANCE-SERVICES	6.00
444110	LUMBER & OTH BLDG MATL-RETL	7.00
452111	DEPARTMENT STORES	7.50

523110	SECURITY BROKERS & DEALERS	8.00
622110	GEN MED & SURGICAL HOSPITALS	8.83
3252	PLASTIC MATL,SYNTHETIC RESIN	9.00
443112	RADIO,TV,CONS ELECTR STORES	9.00
515210	CABLE AND OTHER PAY TV SVCS	9.50
325412	PHARMACEUTICAL PREPARATIONS	9.86
492110	AIR COURIER SERVICES	10.00
311930	BEVERAGES	10.40
445110	GROCERY STORES	10.67
522320	FINANCE-SERVICES	12.00
424210	DRUGS AND PROPRIETARY-WHSL	12.38
452990	VARIETY STORES	13.75
524114	HOSPITAL & MEDICAL SVC PLANS	16.09
446110	DRUG & PROPRIETARY STORES	16.50
324110	PETROLEUM REFINING	18.00
3341	COMPUTER & OFFICE EQUIPMENT	18.33
511210	PREPACKAGED SOFTWARE	20.00
524113	LIFE INSURANCE	20.50
33611	MOTOR VEHICLES & CAR BODIES	23.00
524126	FIRE, MARINE, CASUALTY INS	23.17
334220	RADIO,TV BROADCAST, COMM EQ	29.67
334119	COMPUTER COMMUNICATION EQUIP	30.00
	Overall Average	12.84

Table 5
IS/IT Risk Factor Categorization based on Trust Services Framework

Year	Totals IS/IT Disclosures/Categories	# of factors (maximum of each type per company) Availability	Security	Processing Integrity	Confidentiality	Privacy
2004	18	11 (1)	7 (1)	9 (1)	1 (1)	2 (1)
2005	47	30 (2)	26 (2)	27 (2)	9 (1)	9 (2)
2006	55	28 (2)	28 (2)	24 (3)	12 (2)	9 (1)
	120/232(100%)*	69(30%)	61(26%)	60(26%)	22(9%)	20(9%)

* Individual risk factors may address multiple areas – thus the total number of risk factors is less than the total number of risks by factor.

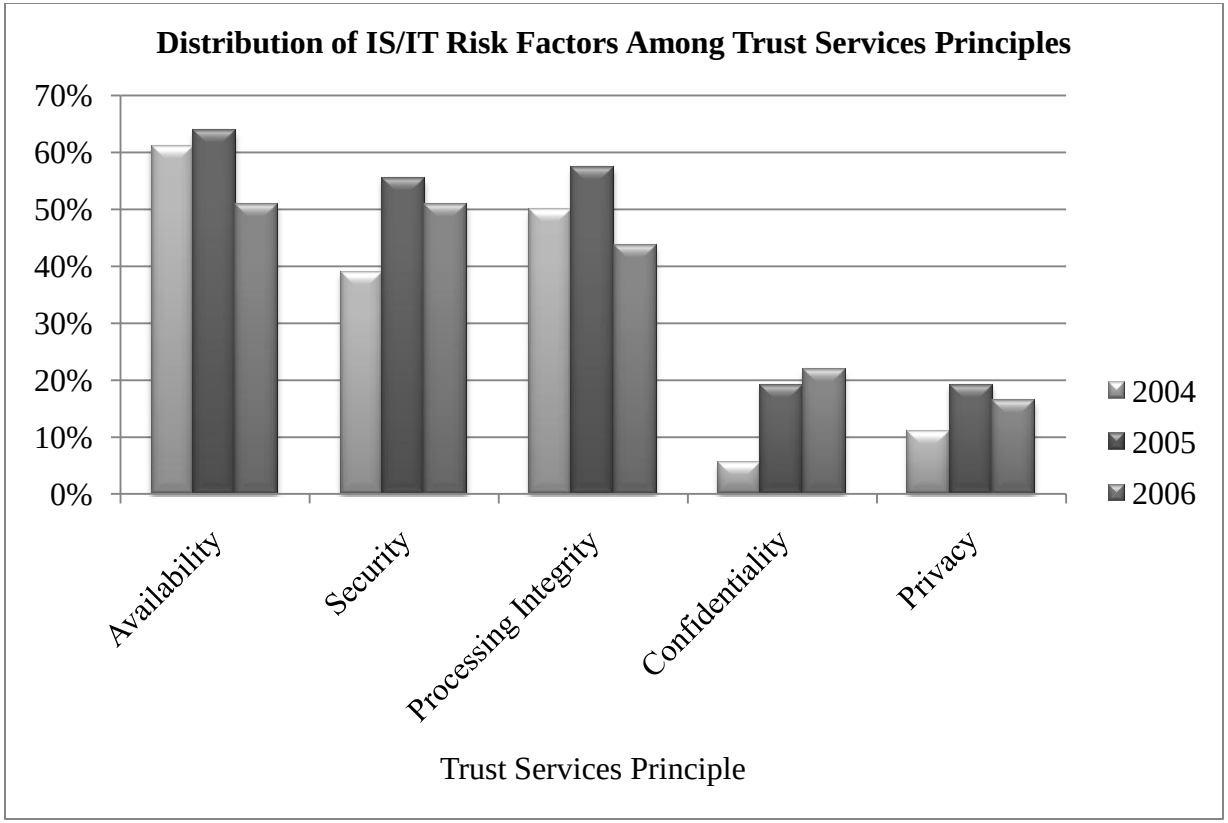
Distribution of IS/IT Risk Factors Among Trust Services Principles
70%
60%
50%
40%
30%
20%
10%
0%
Availability
Security
Processing Integrity
Confidentiality
Privacy
2004
2005
2006
Trust Services Principle

Figure 2