Enterprise Risks, Rewards, and Regulation

Jennifer Blaskovich, Ph.D., University of Nebraska – Omaha, USA
Christopher J. Davis, Ph.D., University of South Florida – St Petersburg, USA
Eileen Z. Taylor, Ph.D., North Carolina State University, USA

ABSTRACT

Risk management is critical to the success of contemporary firms and while new technologies present opportunities for innovation and growth, they present new risks. Risk management of information systems and technology (IS/IT) is particularly critical because firms in almost all sectors of the economy are so dependent on it. We explore firms' response to IS/IT risk management by analyzing their SEC-mandated regulation S-K risk disclosures. We find a lower than expected incidence of risk disclosures related to IS/IT and surmise that this result may be symptomatic of tension between firms' need to comply and their need to appear to comply with the regulation, while at the same time presenting data that are valid, but which do not jeopardize potential investment. We explore three propositions related to IS/IT risk disclosures and discuss implications for research and practice.

Keywords: Enterprise Risk; Risk Management; IS/IT; S-K Risk Disclosures

INTRODUCTION

Risk and reward in the development and use of information systems and technology (IS/IT) are both high. As IS/IT become ubiquitous, more powerful, and less costly, both business and society generally become increasingly dependent upon them. Rapid innovation in IS/IT combined with falling costs affect the potential risk and reward. Lower costs prompt more aggressive investments in newer technologies. Lower costs also affect perceptions of risk: no longer are functionally sophisticated IS/IT the exclusive possessions of corporate giants. Newer technologies like social networking, server and process virtualization and cloud computing present opportunities for rapid innovation. They also come with new, sometimes unrealized risks.

The rapid changes present a significant challenge to those charged with managing risk and rewards. Accounting practice has evolved to finesse the processes and metrics used to manage reward: however, the field of risk management is less mature. At the enterprise level, risk management primarily involves the identification and evaluation of risks to the business. Emerging enterprise risk management (ERM) strategies facilitate intervention to identify, evaluate, mitigate, and report risks.

In this study, we investigate the effect of the SEC's Regulation S-K on risk disclosures made by pubic firms, and discuss how the disclosure process influences the greater area of risk management. We offer three propositions that address those effects and use empirical data to test them. Our focus is on IS/IT, as it provides the physical and logical infrastructure for more and more sectors of the economy, and thus we can reliably expect that all firms face risks in this area. Our analysis reveals that over 40% of Fortune 100 firms reported no IS/IT risks in either of the two years that risk disclosure was voluntary or in the first year that it was mandated by Regulation S-K. Additionally, nearly half of the industries represented in our sample had no firms list even one IS/IT risk factor. We contend that these findings are incongruous with industry reports and research indicating much greater IS/IT risk exposure facing organizations (e.g., Cavusoglu et al., 2004; Hines, 2007; Hodge, 2007; Romney & Steinbart, 2009; Kieke, 2006).

Our paper proceeds as follows. First, we outline prior research into enterprise risk management, information systems governance, and Regulation S-K. From this review, we develop our propositions and set out our research design. Subsequent sections present our results and provide commentary on our findings, observations, and opportunities for future research.

ENTERPRISE RISK MANAGEMENT AND TODAY'S IS/IT RISKS

Enterprise Risk Management (ERM) comprises a multi-step process of risk identification, evaluation, mitigation, and reporting. The aim of the process is to call attention to areas where management might intervene or institute additional oversight to ameliorate risk and prevent future losses; however, firms do not always recognize or realize the benefits of ERM. Beasley et al. (2009) reports that 62% of 700 for-profit, not-for-profit, and governmental entities surveyed indicate that *(although)* the volume and complexity of risks had increased substantially in the last five years, "…not all organizations are modifying their procedures for identifying, assessing, managing and communicating risk information to key stakeholders". Also lacking is the development of a new organizational mindset that recognizes the wide variety of risks present in business. While some risks may be adequately addressed (i.e., market and credit risks for banks), there is a "real danger" that other types of risks are ignored (Maurer, 2009, 13). Critical to the success of contemporary business, information systems present challenges to risk management that have attracted attention both within the development and user communities and among regulators.

Contemporary firms are so dependent on IS/IT that those systems have become 'mission critical'. Increasingly rich electronic media support increasingly complex interactions and exchanges within and between firms. Today IS/IT support complex and continually evolving business processes: every facet of the firm from purchasing to accounting, production, sales, distribution, and logistics all depend on the efficient and effective operation of IS/IT. Growing dependence on the World Wide Web and web 2.0 capabilities such as server virtualization and cloud computing have further increased the complexity of both the processes and the technologies that support them (Sherer & Alter, 2004). Clearly, as business processes become increasingly interdependent and information intense, the risks associated with their failure or other interruption of services increase in complexity and volume. Regulatory compliance is also highly dependent on the proper functioning of IS/IT. Studies show that IS/IT is the most complex and costly to document in Sarbanes-Oxley compliance efforts, and that it should be considered a "high risk" area (Bryan, 2009, 34). The identification, assessment, and communication of risk is recognized as the core of effective IS/IT governance (O'Leary, 2000; Hunton et al., 2004; Cavusoglu et al., 2004). Recent business failures have raised awareness of the risks surrounding IS/IT: inadequate controls have been cited as a significant risk factor (Solomon, 2005; Bryan, 2009). Such risks have been recognized by the U.S. government: in May 2009, President Obama created the role of cyber security czar to protect the nation's digital infrastructure (Simpson & Cole, 2009). Highly publicized data theft incidents, as experienced by companies such as TJX and Heartland Payment Systems, have served to intensify the spotlight on IS/IT risk exposure (Acohido, 2009; SecurityFocus, 2007).

REGULATION S-K AND PROPOSITION 1

Regulation S-K was one result of the SEC's intention to alert investors to the wide-ranging risks of purchasing and owning a company's stock. Enacted in 2002, the regulation requires that companies disclose the most significant factors that may adversely affect the issuer's business, operations, industry, financial position, or its future financial performance (Oppenheimer et al., 2005). In the financial services sector, the SEC has (since 1997) required firms to disclose information about market risk exposures from financial instruments (Securities and Exchange Commission, 1997). However, the corporate accounting scandals and business gyrations of the early 2000's show clearly that firms face a multitude of other risks: many of these arise from the dependence of business processes on IS/IT. Regulation S-K mandates the communication of an organization's broad risk exposure, and applies to all public companies. It seems likely that firms who were not engaging in effective risk management prior to the regulation may begin to implement and improve their risk management programs in response to the regulation.

Because IS/IT are mission critical, one might expect firms to identify and disclose myriad IS/IT related risks. However, we have identified four factors from prior research that may adversely affect comprehensive identification and disclosure.

- Firms may inadequately identify IS/IT risks
- Firms may not appreciate the interconnectivity and synergy of IS/IT risks

- Firms may not see any benefit in disclosing those risks (and may in fact see negative outcomes)
- Firms may view Regulation S-K not as a mandate to perform ERM, but merely as a burdensome compliance task, influenced by myriad legal and other pressures.

We posit that the first factor, inadequate identification of IS/IT risks, arises due to the absence of consistent and coherent guidance on risk identification. Despite their substance and widespread adoption, IT governance frameworks such as COBIT, ITIL and ISO/IEC 17799 do not specifically provide guidance for assessing or addressing intra- or inter-organizational concerns and risks associated with the complex business processes supported by IS/IT (Sutton et al. 2008). ITIL provides guidance on best practices for IT service management; COBIT is primarily a high-level governance and control framework, and ISO/IEC17799 provides a framework for information security management. Their emphasis of events and other circumstances internal to the firm limit their capacity to accommodate the more emergent risk factors and the inter- and intra-organizational dependence on IS/IT that generate them.

Relatedly, uneventful business operations may lull management into a false sense of security when it comes to their systems, leading them to underestimate and operate unaware of the critical risks they face. Prior research shows that user communities and management tend to take IS/IT for granted. Sophisticated and successful operational use leads to an unrealized and largely underestimated dependence on IS/IT (Kieke, 2006). The risks associated with their failure do not take center stage when they are working smoothly. We surmise that organizations may be operating under a false sense of security whereby mission criticality is masked by the uneventful normal operation of IS/IT. Dependence is so complete that IS/IT becomes part of the undiscussed social routine, until the wheels come off.

The second factor, failure to fully appreciate the variety and synergistic potential of the IS/IT risks that are identified, is highlighted by Dehning et al. (2005), who caution against the narrow conceptualization of IS/IT risks, primarily because these risk factors are difficult if not impossible to measure directly. If management bases its decisions on a narrow and consequently rather naïve assessment of specific individual factors, the cumulative and consequential effects of such risks can be missed (*op cit*, 1004), giving rise to and perpetuating a vicious circle: underestimation leading to underreporting of risks.

The third factor takes a cost/benefit approach and presumes that firms will not see any good coming from disclosing these risks. Zimmerman (1987, 131) observes "…despite the apparent unanimity of interest in and high value placed on risk communication, considerable disagreement occurs with respect to its goals or purpose." Certainly, if managers are aware of the risks, it may be difficult to see the benefit of sharing these Achilles' heels with the public. They may overlook the goodwill generated among investors should these disclosures demonstrate a commitment to transparency to the public. Managers may see only costs and negativity should they disclose these risks. They may fear that investors will view their firms not as open and honest, but as an unsafe investment – one burdened with risk. Outcomes arising from disclosure of IS/IT risks include negative market reaction or overreaction, display of weakness to competitors, and broadcasting of security weaknesses to potential hackers (Suijs, 2007; Linsley & Shrives, 2005; Securities and Exchange Commission, 2011)

The last factor that may impede firms from implementing a comprehensive risk program is that they view the regulation as a compliance issue, rather than as an opportunity to enhance their business. This view focuses on satisfying the SEC by coming up with a list of plausible, generic risk factors that ostensibly meet the requirements of the regulation. A surface-only approach ignores the true value that firms can gain from a complete ERM implementation; however, given limited resources, it is one they might well choose.

Thus, while we expect that the regulation will lead to improvements in the identification and disclosure of IS/IT risks, several factors may counter this expectation. At the same time, the nearly complete dependence of contemporary business on IS/IT, the ever increasing media coverage of IS/IT failures, and the requirements of Regulation S-K should demand that organizations pay attention to IS/IT risks. Accordingly, our first proposition is as follows:

P1 Pervasive dependence on IS/IT will increase the volume of IS/IT risks identified, and thus disclosed in response to regulation S-K.

TRUST SERVICES FRAMEWORK AND PROPOSITION 2

As noted earlier, dependence on IS/IT goes unnoticed, as long as all is working smoothly. By requiring firms to identify and disclose risks, Regulation S-K may provide the impetus for a thorough review of these systems. Several comprehensive governance frameworks are available to guide managers in conducting IS/IT risk assessments.

The Trust Services Framework (TSF), developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), provides a robust typology of risks. TSF comprises a set of core principles and criteria that directly address the reliability of a firm's information technology and systems (AICPA & CICA, 2006). TSF provides a means to accommodate and categorize risk disclosures from firms and industries throughout the economy. The five fundamental TSF principles are security, availability, processing integrity, confidentiality, and privacy. Security is the foundational principal of the framework on which the other four depend (Romney & Steinbart, 2012). These five principals characterize controls and policies designed to identify and attenuate risk to both IS/IT operations and development processes. 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 confidential firm information, and privacy focuses on the protection of information a firm 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 & CICA, 2006). The professional guidance for identifying and addressing risks provided by TSF (Coe, 2005) makes it a strong candidate for firms to use when assessing their IS/IT risks. Thus, although other frameworks are available, TSF offers a robust yet parsimonious tool for our analysis.

The existence of these (and other) frameworks provides a blueprint for managers to use when faced with identifying risks and developing risk disclosures. Regulation S-K motivates firms to seek out and implement these frameworks; the comprehensiveness of these frameworks increases the likelihood that management will identify a larger and more varied set of risk factors.

P2 Regulations requiring the identification and disclosure of risk factors increase firms' awareness of the variety of IS/IT-related risk factors facing them.

Today, few firms are immune to IS/IT risks. In the past, only certain limited sectors were high-risk (e.g. medicine, defense, and the airlines); now, IS/IT dependence is critical to the success of the majority of sectors in the economy (Cavusoglu et al., 2004). The proliferation of IS/IT has been particularly significant in the financial services sector (Zhu et al., 2004). As noted previously, this sector has been subject to risk disclosure regulation since 1997, and thus, it is reasonable to expect that some level of risk awareness and management is present. Research indicates, however, that 60% to 90% of all firms have experienced a major control failure or IS/IT security breach (Cavusoglu et al., 2004; Romney & Steinbart, 2009; Kieke, 2006; Hines, 2007). This reality indicates that most all firms have some IS/IT risk exposure, which may or may not have been recognized before the failure.

Clearly, there are variations both within and between industry sectors. Amazon.com is more dependent on IS/IT than more traditional bricks and mortar retailers, and farming less so than telecommunications. Nevertheless, the apparently inexorable rise of e-commerce, whether business-to-business or business-to-consumer, inevitably gives rise to a growing range of IS/IT risks for all industry sectors. IS/IT have become mission critical for a significant proportion of businesses in all sectors of the economy. Regulation S-K applies to all industry sectors and may, therefore, motivate firms to identify IS/IT risks not previously considered. Our third proposition addresses this expectation:

P3 Regulations requiring the identification and disclosure of risk factors increase the awareness of IS/IT risks by firms across all industry sectors.

METHOD

In order to test our propositions we evaluated the nature and scope of IS/IT risks disclosed in response to the S-K mandate. We first identified IS/IT-related risks and their position (relative to other risks) within firms' annual reports. We then classified the identified and ranked risks into the five substantive categories included in the Trust Services Framework (TSF). In the third and final step, we used industry codes to explore the relationship between IS/IT-risk disclosure and industry sector as a means to test our last proposition.

ANALYTICAL APPROACH

We identified the Fortune 100 firms (ranked according to total sales) for the year 2004 (listed in Appendix A) and collected relevant data from the Compustat database. We excluded five mutual insurance firms since they are not publicly traded: the first phase of our analysis began with an initial pool of 95 firms. We analyzed the records of these 95 firms over the three years 2004-2006. Various mergers further reduced our initial data set from 95 firms to 93 in 2005 and 92 in 2006 (the first full year of implementation). For this analysis, the 280 10-K reports were used to gather industry code and text of item 1a (the location of the risk factor disclosures required by Regulation S-K).

We categorized the textual data in two stages. First, we isolated IS/IT-related disclosures, then, we classified them using the principles embodied in the TSF (the coding scheme used is presented in Appendix B). Inter-rater agreement for the first phase was 97.2% and 87.3% for the second. Inter-rater reliability was Kappa = 0.941, a very high level of agreement (Landis and Koch, 1977). Differences between coders were resolved through review and discussion between them and an independent expert in information systems.

We then calculated the average position of the IS/IT-related disclosures relative to non-IS/IT-related disclosures. This aspect of our analytic approach was a response to the substantial challenges of developing measurement models for risk assessment identified by Debreceny (2006) and others. Clear distinction between levels of risk has intuitive appeal as highlighted by a study of the COBIT framework (Debreceny, 2006). Regulation S-K makes no mention of degree or importance of risks, nor does it require firms to specifically rate or rank risks. Thus, it provides no definitive method of judging the level of each risk relative to other risks. We compensated for this limitation by using the position (rank) of each classified disclosure in relation to others in Item 1a of the 10-K report: positional data such as rank provide a reasonable surrogate indicator of significance.

RESULTS

We identified 3,795 individual risk factors from the 280 documents analyzed. In 2004, only 68% of firms in the data set (65/95) reported one or more risk factors. This proportion rose to 100% in 2005 and continued at this level through 2006. During this period, the average number of risk factors per firm per year increased slightly, from 13.28 in 2004 to 16.27 in 2006, as did the maximum number of risks per firm, from 41 to 48. Table 1 illustrates these trends.

Table 1
Total Risk Factors by Year

	Number of risk factors	Number of firms reporting at least one risk factor	Mean number of risks per firm	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

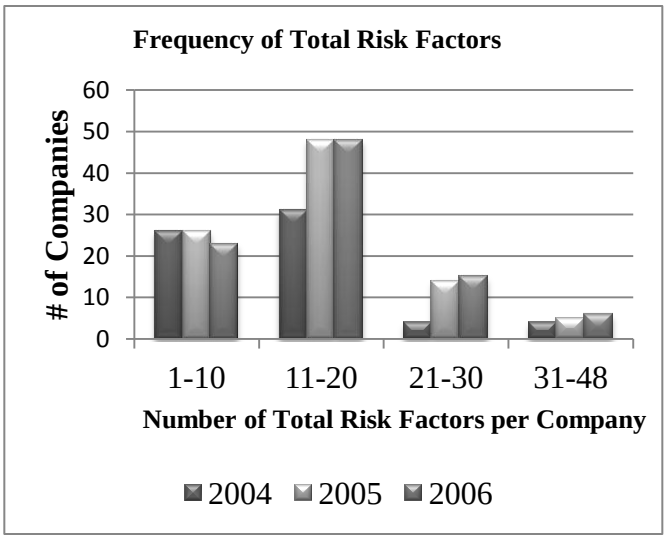

Figure 1

Figure 1 presents a frequency distribution of these data. Although the upward trend is evident from the visible steps in the 11-20 and 21-30 ranges, we noted the very modest increase in the number of registrants reporting higher numbers of risk factors over time.

Proposition 1: Pervasive dependence on IS/IT will increase the volume of IS/IT risks identified, and thus disclosed in response to Regulation S-K

The global data for all risk factors summarized above show that all firms reported at least one risk by the first full year of S-K implementation. However, the disclosure of IS/IT-related risks was relatively low. Only 18 firms reported one or more IS/IT risk factor in 2004, 47 in 2005, and 55 in 2006: Table 2, Panel A provides an overview of this trend. The steady increase in the total number of risk factors reported (Table 1) seems mirrored here by an increase in the number of firms reporting at least one IS/IT risk factor. In 2004 (the year before the mandate), only 27.6% of Fortune 100 Regulation S-K eligible firms reporting risk factors reported *any* IS/IT risk factors. The proportion increased to 50.5% in 2005, and 59.8% in 2006. Nevertheless, we were surprised by the absence of any IS/IT risk factor disclosure from over 40% of the largest firms filing under Regulation S-K in 2006 (the first full year of the regulation).

Table 2, Panel B presents the result of our analysis of the relation between the number and percentage of IS/IT-related disclosures to all risk disclosures. Although the number of risk disclosures overall increased, those related to IS/IT represented a relatively small proportion (3.6% of all risks disclosed over the three year period). This proportion has remained relatively static, increasing from 2.1% of the total number of risk factors disclosed in 2004 to 3.6% in 2005 and 4.4% in 2006.

These proportions are inconsistent with the dependencies and risks outlined in the introduction and the centrality of risk identification, assessment, and communication to management and governance of IS/IT. Our analysis shows that the proportion of IS/IT risk factor disclosure *has* increased: however, this increase is from such a *very* low initial threshold that is impossible to reconcile the increase with prior research into IS/IT risks and failure (Charette, 2005), which suggests large increases in IS/IT risk over the same period.

Table 2, Panel B extends this analysis to summarize the positional (ranking) data we used as a proxy indicator of the significance of the risks disclosed: the average rank of non-IS/IT risks factors is 10.5, the average rank for IS/IT risk factors is 13.0. This analysis suggests that IS/IT risks appeared consistently later in the risk disclosures, suggesting that management considered them less significant than other risks. Once again, this seems counter-intuitive in the context of prior research and experience of IS/IT failures.

Based on the low incidence of reported IS/IT risks, and their later appearance in risk disclosures, and in light of only slight increases in the number of IS/IT risk factors disclosed, Regulation S-K has not appeared to improve identification and disclosure of IS/IT risk factors. We do not find support for P1.

Table 2
Prevalence of IS/IT Risk Disclosures

Panel A

Year	Number of firms reporting at least one IS/IT risk	Total number of firms reporting at least one risk factor	%age of firms reporting at least one IS/IT risk
2004	18	65	27.6%
2005	47	93	50.5%
2006	55	92	59.8%

Panel B

	Year	Number of individual risks	%age 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	51	3.6	12.4
Non-IS/IT Risks	2005	1384	96.4	10.4
Total	2005	1435	100	
IS/IT Risks	2006	66	4.4	13.1
Non-IS/IT Risks	2006	1431	95.6	10.9
Total	2006	1497	100	
IS/IT Risks	Total	135	3.6	13.0
Non-IS/IT Risks	Total	3660	96.4	10.5
Total	Total	3795	100	

Proposition 2: Regulations requiring the identification and disclosure of risk factors increase firms' awareness of the variety of IS/IT-related risk factors facing them.

This proposition addresses the distribution of IS/IT risks among the various risk areas. As noted earlier, several frameworks exist to assist firms in assessing IS/IT risks. COBIT, for example, derives 215 specific control objectives from 34 high-level IS/IT processes, which provides a comprehensive, yet highly detailed blueprint. TSF provides five general categories of IS/IT risks, which, given the content and number of risk factors in our population, provided a parsimonious yet sufficient tool for our analysis.

Recall that the five fundamental principles TSF includes are security, availability, processing integrity, confidentiality, and privacy. TSF is a comprehensive instrument: guidelines for its use require that all five principles are a pre-requisite for systems reliability; yet, experts agree that entirely eliminating the risks accommodated by TSF is impossible (Romney & Steinbart, 2009). A benefit of TSF's comprehensive nature is that it can accommodate any and *all* risks identified. A drawback of this is that the classifications in our coding schema (Appendix A) are not mutually exclusive: 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). Consequently, we include some risks in more than one category.

The summary presented in Table 3 shows that issues relating to system availability represent a significant proportion of the IS/IT-risks disclosed, 29.7% of the total number of risk factors classified (232). Security was the next most significant factor according to this classification with 61 disclosures (26.2%), followed by processing integrity issues (25.8%), threats to confidentiality (9.5%) and privacy (8.6%).

Table 3
IS/IT Risk Factor Categorization based on Trust Services Framework

Year	Totals IS/IT Disclosures/Categories	# of factors (maximum of each type per firm) 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%)

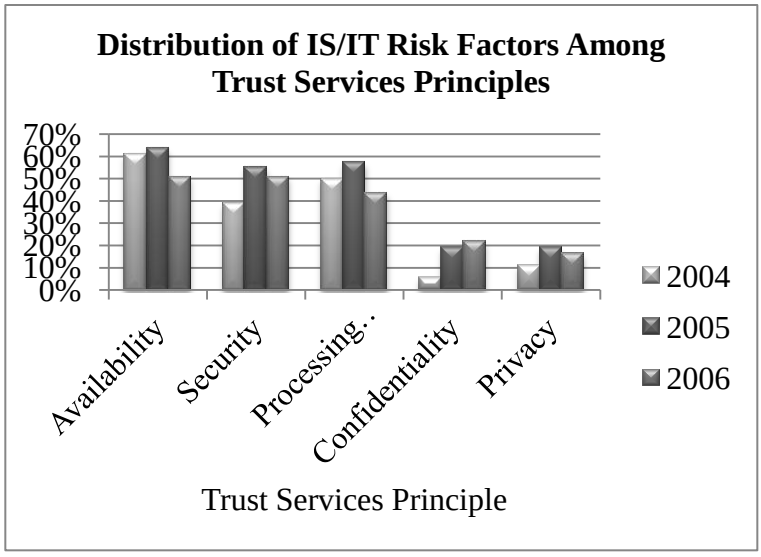

Figure 2

Changes in the distribution of these risk factors over time (Figure 2) show that disclosure of confidentiality and privacy risks increased as a percentage of total IS/IT risk factor disclosures over the three-year period.[1] This trend indicates an increase in corporate awareness of these two types of IS/IT risks, providing support for our proposition that the regulation has improved understanding of the variety of risks facing firms. There appears to be some rebalancing of IS/IT risks reported.

Proposition 3: Regulations requiring the identification and disclosure of risk factors increase the awareness of IS/IT risks by firms across all industry sectors.

In the third phase of our analysis, we reviewed variations between industries to test our proposition about the frequency and proportion of IS/IT risks disclosed. Our expectation was that firms in industries with greater reliance on and pervasiveness of IS/IT would report greater numbers (and/or a greater proportion) of IS/IT risks than firms in industries with less reliance on IS/IT. Table 4 lists the specific industries in which *at least one firm* reported IS/IT risks *as at least 10%* of their total risks reported (2004-2006). Of the 56 industries in our data set, only six industries surpassed this threshold. Table 4 shows these six industries in descending order of the percentage of total risk factors that are IS/IT-related: finance (25%), radio, TV, and electrical stores (25%), department stores (13.3%), hospital and medical service plans (12.4%), general medical and surgical hospitals (11%), and plastics (1%).

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

Some of our findings appear to support P3. Finance firms and hospital and medical service plans, whose operational processes depend heavily on IS/IT and are closely regulated, made the top of the list. Some retail stores (radio, TV, electrical and department) which depend on IS/IT to support operational processes central to revenue generation, purchasing, record keeping, and distribution also reported greater numbers and percentages of IS/IT risks. We expect regulation and dependence makes IS/IT risks 'present' in the minds of managers and thus makes identification and disclosure more likely.

However, the finding that 50 industries out of the 56 analyzed (some 89%) list fewer than 10% of their risks as IS/IT-related was surprising. Telecommunications, insurance, oil and gas, pharmaceuticals, and computers (including software) were included in the 'less than 10%' category. While we acknowledge that firms in these industries might be well placed to mitigate some IS/IT risks through avoidance or sharing, and that these firms may face a multitude of other risks, the proportion of IS/IT risks to total risks was surprising and at odds both with our proposition and the expectations that arise from prior research and experience.

Further, we are at a loss to explain why 27 industries (48%) had *no* firms list even a *single* IS/IT risk. These industries include computer programming and data processing (106), public warehousing (86), guided missiles and space vehicles (51), television broadcasting (50), and meatpacking (43) – figures in parentheses show the total number of risk factors disclosed in Item 1a for 2004-2006. While the variations in the level of IS/IT dependence between industry sectors should affect the volume of risks identified and disclosed, our analysis reveals a rather alarming lack of consistency that merits further investigation.

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

NAICS	Industry Description	Average IS 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

In a supplemental analysis, (see Table 5) we summarized variations between industry groupings using positional (rank) data as a surrogate indicator of significance to provided additional insight into industry differences. Lower values (towards the top of the table) indicate risks that appear 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.

This phase of our analysis shows that the relative significance of risk disclosures varies between industry sectors: however, we discern no consistent pattern. Support for our proposition is equivocal.

Table 5
Specific Industries with Firms 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)	%age 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%

DISCUSSION & CONCLUSIONS

The SEC designed Regulation S-K to improve risk communication by firms to investors and other external stakeholders. A necessary precursor to this communication is the identification and evaluation of risks by firm managers and accountants. Our results lead us to question whether the regulation provides a means to demonstrate visible compliance rather than effective risk management – a nod to communication, without full evaluation or intervention. Consequently, we question the value of Regulation S-K to stakeholders. Are managers implementing effective enterprise risk management procedures and communicating the results to the public, or is Regulation S-K an exercise in compliance?

Our first proposition states that pervasive dependence on IS/IT and high levels of regulation will increase the volume of IS/IT risks identified, and thus disclosed in response to regulation S-K**.** Given what we know about IS/IT risks facing firms in the current technological environment, we expected to observe a number of IS/IT-related risk disclosures within firms' annual reports, in response to Regulation S-K. We observed that over 40% of Fortune 100 firms reported no IS/IT risks in either of the two years that risk disclosure was voluntary, and more telling, that this percentage held in the first full year that that the regulation was mandated. Regardless of the diligence of managers and IS/IT professionals, no system can be made 100% secure, making some exposure to IS/IT risk unavoidable (Bodin, Gordon, & Loeb, 2008). Granted, as discussed earlier, firms may indeed have implemented effective risk management programs, yet have chosen to keep their findings private, thus preventing us from observing results. However, if this is the case, Regulation S-K has not accomplished its mission of improving the flow of information to investors and other external stakeholders.

Our second proposition states that regulations which require the identification and disclosure of risk factors increase firms' awareness of the variety of IS/IT-related risk factors facing them. We tested this proposition by exploring the variation in the types of IS/IT risks disclosed. Using the five TSF principles as a classification system, we found that two areas, confidentiality and privacy, were increasing as a proportion of total IS/IT risks reported over time. This observation supports increased awareness of these two areas. We did observe declines in the proportion of risks related to availability, security, and processing integrity, however, because the absolute number of IS/IT risks increased, increased awareness of the other two areas did not come at a cost to these three areas.

Our analysis of the variation in IS/IT risks finds that threats to availability of systems are reported most often. Since so many business processes rely on IS/IT, availability is critical. In IS/IT-dependent business sectors such as financial services and healthcare, 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, we perceive system availability to be the most significant and prior research (Meall 2009) supports this perception. 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. First, the rate of change in the number of these risk factors over time (see Table 2) suggests persistent under-reporting. Second, we find it difficult to comprehend how managers within industries that are ostensibly "risk free" in regards to IS/IT according to their disclosures – including computer programming and data processing, and guided missiles - are failing to acknowledge their dependence on IS/IT to support mission critical business processes. This issue is addressed in our third proposition, that Regulation S-K will increase IS/IT risk disclosure across industries.

We cannot support the assumption that firms believe they have mitigated the risk: a recent study found that 69% of business leaders indicate that threats to IS/IT continuity represent a clear and present danger (Hodge 2007).We conclude that the risks themselves have been insufficiently analyzed in-house and are therefore under-appreciated, evidenced by the low rate of reporting. This observation concurs with Benaroch et al. (2006) who found that managers in a financial services setting relied on intuition to assess IS/IT investment risk rather than on any formal method or framework.

One explanation for the scarcity of IS/IT risk factor disclosures is that Regulation S-K serves the needs of representation before those of intervention. In other words, firms are merely complying with a directive, rather than embracing a new process (enterprise risk management). Firms enact compliance with Regulation S-K by aligning their actions with those of firms in their own or a similar industry (Miller and O'Leary 2007), meeting the technical requirements of their regulators, or addressing the demands of their market.

Such behavior gives rise to conceptualization of regulations as what DiMaggio and Powell (1983) call an 'iron cage'. Regulation promotes institutionalization and bureaucratization, which becomes a powerful means of controlling individuals, to such an extent that it acts as a cage rather than a rationalist organizing framework or form (Weber 1952). Individual thought becomes imprisoned in the need to 'box-check', audit reports default to standardized formats, and firms rigidly conform to rituals prescribed by the state, professions, and competition (Power 2009; DiMaggio and Powell 1983). Our findings provide some evidence that disclosures made in response to Regulation S-K reflect regulatory compliance more so than a holistic risk management strategy.

We have examined the effects of Regulation S-K on IS/IT-related risk disclosures, and in doing so add to our understanding of its strengths and limitations. The strength of regulatory uniformity arises from codification 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. The uniformity and codification of S-K and other regulatory instruments become an end rather than a means to an end. In this situation, regulatory instruments can act like cages rather than frameworks.

This outcome may be symptomatic of tension between the need to comply and the need to appear to comply with the regulation, while at the same time presenting data that are valid, but which do not jeopardize potential investment.

What is clear from the disclosure practices we report is 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 a firm. The archival data used to test our propositions cast doubt on whether firms are truly *informing*: identifying risks, exploring their causes and effects, putting in place 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. If, as Power (2009) observes, risk management is less about managing risk and more about gaining institutionalized legitimacy, should we not expect the same from risk management disclosure?

Future research should explore the connections (or lack thereof) between firms' established enterprise risk management processes and their S-K risk disclosures. Questions may include, '*who creates and approves the risk disclosure?'* and '*how much does the disclosure change from year-to-year in response to new risks identified or old risks mitigated?'* Behavioral analyses using interviews and surveys would be appropriately rich methodologies for these explorations.

Further research might adopt a 'user' or consumer perspective, asking investors whether they read risk disclosures, and if they do how those disclosures influence their investing decisions. *If investors are not using risk disclosures, is it due to a lack of awareness that they exist, a lack of trust in their veracity, or a lack of useful information provided?* For example, if there is no differentiation in risk factor disclosures among competing investments (firms), then the value-relevance of the disclosure for investment decisions is nil. To answer questions about the variety of risk disclosures will require extensive analysis, but should prove fruitful.

Further research might also explore the value of risk disclosures 'post-event.' In other words, *does the disclosure of specific risk factors lessen legal liability in shareholder lawsuits?*

Overall, research that addresses the effectiveness of Regulation S-K is clearly worthwhile and timely. Results and conclusions would, we anticipate, highlight a rather naïve sense of security in the published disclosures and inform the SEC and government regulators about the efficacy and value of this regulation, and may provide the impetus to managers to take a closer look at risk management within their firms.

Finally, we suggest that our study demonstrates the potential and wider applicability of the notion of mediating (Miller and O'Leary, 2007) or, perhaps, 'remediating' instruments. Such a perspective provides a warning to risk managers that mimicking peers may leave you exposed to unidentified risks: it is unrealistic to rely on others to disclose or even to identify risks. It also reiterates the mutual dependence of representation and intervention, raising questions that prompt even deeper review of regulations and their effectiveness - did the SEC intend this outcome? Do significant and serious risks remain unidentified or undisclosed – and can we tell? Does the current risk disclosure process help the firm *and* the investing public?

AUTHOR INFORMATION

Jennifer Blaskovich, PhD., CPA is an Associate Professor at the University of Nebraska – Omaha. She worked as an auditor in public accounting prior to entering academia. Jennifer researches decision-making issues surrounding accountants and information systems, publishing in *The Journal of Applied Business Research*, *The Review of Business Information Systems*, *The CPA Journal*, and the *Journal of Information Systems*. E-mail: jblaskovich@unomaha.edu. Corresponding author.

Christopher J. Davis, PhD is an Associate Professor at the University of South Florida – Saint Petersburg. He worked at HP Labs and in a number of development and management roles in the public and private sector before moving into academia. His research into process management has been published in a range of journals including *Communications of the ACM*, *Information Management*, *the International Journal of Technology and Human Interaction*, *Systems Research and Behavioural Science*, the *Journal of Computer Information Systems*, the *Journal of Organizational Change Management* and the *MIS Quarterly*. E-mail: davisc@usfsp.edu

Eileen Z. Taylor, PhD., CPA is an Associate Professor at North Carolina State University. She worked in public and private accounting. Her research on ethics and whistleblowing has appeared in the *Journal of Business Ethics* and *Journal of Accounting and the Public Interest*. She has published work on XBRL in *Accounting Horizons*, the *Journal of Accountancy*, and *Financial Executives International*. E-mail: eileen_taylor@ncsu.edu

REFERENCES

1. Acohido, B. (2009, January 20). Hackers breach Heartland Payment credit card system. Retrieved October 18, 2011, from USA Today: http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm

2. AICPA and CICA. (2006). 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.
3. Beasley, M., Branson, B., & Hancock, B. (2009). Report on the Current State of Enterprise Risk Oversight. Raleigh, NC: ERM Initiative at North Carolina State University.
4. Benaroch, M., Lichtenstein, Y. & Robinson, K. (2006). Real options in information technology risk management: An empirical validation of risk-option relationships, *MIS Quarterly* 30 (2), 827-864.
5. Bodin, L., Gordon, L., & Loeb, M. (2008). Information Security and Risk Management. *Communications of the ACM, 51*(4), 64-68.
6. Bryan, L.D. (2009). Corporate managers' experiences related to implementing Section 404 of the Sarbanes-Oxley Act: A focus on information systems issues. *The Journal of Applied Business Research*, May/June, 25 (3): 25-35.
7. Cavusoglu, H., Cavusoglu, H., & Raghunathan, a. S. (2004). Economics of IT security management: Four improvements to current security practices. *Communications of the AIS, 14*, 65-75.
8. Charette, R. N. (2005). Why Software Fails. *IEEE Spectrum, 42*(9), 42-49.
9. Coe, M. J. (2005). Trust services: a better way to evaluate IT controls. *Journal of Accountancy* 199(3), 69-75.
10. Debreceny, R.S., (2006). Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls, Hawaii International Conference on System Sciences, p. 196c, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 8.
11. Dehning, B., Richardson, V.J., and Stratopoulos, T. (2005). Information technology investments and firm value, *Information & Management* 42 (7): 989-1008.
12. DiMaggio, P., & Powell, W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48*(April), 147-160.
13. Hines, M. (2007). Report: 90 percent of companies fail compliance. Retrieved October 17, 2011, from Infoworld : http://www.infoworld.com/t/business/report-90-percent-companies-fail-compliance-223
14. Hodge, N. (2007). Boards fail to grasp IT risk. *Financial Director*, 46.
15. Hunton, J., Wright, A., & Wright, S. (2004). Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems, 18*(2), 7-28.
16. Kieke, R. (2006). Survey shows high number of organizations suffered security breach in past year. *Journal of Health Care Compliance, 8*(5), 49-68.
17. Landis, J., & Koch, G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*, 159-174.
18. Linsley, P., and P. Shrives (2005). Disclousre of risk information in the banking sector. *Journal of Financial Regulation and Compliance* 13(3): 205-214
19. Maurer, F. (2009). Creating value through enterprise risk management. *The Journal of Applied Business Research*, May/June, 25 (3): 13-24.
20. Meall, L. (2009). Flirting with disaster. *Accountancy* 143(1390), 59-60.
21. Miller, P. and T. O'Leary. (2007). Mediating instruments and making markets: Capital budgeting, science and the economy, *Accounting, Organizations and Society* 32 (7-8): 701-734.
22. O'Leary, D. (2000). *Enterprise Resource Planning Systems: Systems, Life Cycle, Electronic Commerce, and Risk.* Cambridge, MA: Cambridge University Press.
23. Oppenheimer, Wolff, and Donnelly, LLP. (2005). SEC Alert 12/1/05: Required new risk factor disclosure in form 10-Ks and 10-Qs.
24. Power, M. (2009). The risk management of nothing. *Accounting, Organizations, and Society* 34 (6/7), 849-855.
25. Romney, M., & Steinbart, P. (2009). *Accounting Information Systems* (11th edition ed.). Upper Saddle River, NJ: Pearson Education Inc.
26. Romney, M., & Steinbart, P. (2012). *Accounting Information Systems* (12 th edition ed.). Upper Saddle River, NJ: Pearson Education Inc.
27. Securities and Exchange Commission. (1997). Financial Reporting Release No. 48. Washington, D.C.: U.S. Securities and Exchange Commission.
28. Securities and Exchange Commission. (2011). CF Disclosure Guidance: Topic No. 2 Cybersecurity. Washington, D.C.: U.S. Securities and Exchange Commission.

29. SecurityFocus. (2007, May). TJX Theives exploited wireless insecurities. Retrieved October 18, 2011, from securityfocus.com: http://www.securityfocus.com/brief/496
30. Sherer, S., & Alter, S. (2004). Information systems risks and risk factors: Are they mostly about information systems? *Communications of the Association for Information Systems, 14*, 29-64.
31. Simpson, C., & Cole, A. (2009, May 30). Obama Moves to Curb Data-System Attacks. *Wall Street Journal - Eastern Edition*. p. A3.
32. Solomon, D. (2005, March 2). Accounting rule exposes problems but draws complaints about costs. *Wall Street Journal - Eastern Edition*, A1, A12.
33. Suijs, J. (2007). Voluntary disclosure of information when firms are uncertain of investor response. *Journal of Accounting and Economics*, 43 (2/3), 391-410.
34. Sutton, S., D. Khazanchi, C. Hampton, and V. Arnold. (2008). Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B eCommerce Relationships, *Journal of the Association for Information Systems* 9 (3/4): 151-174.
35. Weber, M. 1952. The Protestant Ethic and the Spirit of Capitalism. New York: Scribner.
36. Zhu, K., Kraemer, K., & Dedrick, J. (2004). Information Technology Payoff in E_Business Environments: An International Perspective on Value Creation in the Financial Services Industry. *Journal of Management Information Systems, 21*(1), 17-54.
37. Zimmerman, R. (1987). A Process Framework for Risk Communication. *Special Issue on the Technical and Ethical Aspects of Risk Communication, Science, Technology, & Human Values* 12 (3/4): 131-137.

APPENDIX A

Listing of Firms Studied – 2005 Fortune 100 (based on 2004 reports)

1	Wal-Mart	34	Dow Chemical	67	Sprint
2	Exxon	35	Albertson's (sold to Supervalu on June 2, 2006)[3]	68	New York Life Insurance[1]
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[1]
16	Cardinal Health	49	Motorola	82	Sunoco
17	Altria	50	Intel	83	Mass Mutual Life[1]
18	Bank of America	51	Allstate	84	Merck
19	State Farm Insurance[1]	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)[2]
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)[2]	66	DuPont	99	Nationwide Insurance[1]
				100	Abbott Laboratories

[1]Dropped from original pool (insurance firms)
[2]Merged or failed in 2005
[3]Merged in 2006

APPENDIX B

AICPA Trust Services Principles description used to classify Risk Disclosures

Security	The system is protected against unauthorized access (both physical and logical).
Availability	The system is available for operation and use as committed or agreed.
Processing Integrity	System processing is complete, accurate, timely, and authorized.
Confidentiality	Information designated as confidential is protected as committed or agreed.
Privacy	Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.

APPENDIX C

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 Card member account information in connection with our charge and credit cards. Criminals are using increasingly sophisticated methods to capture various types of information relating to Card members' 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.

NOTES

