The International Journal of Digital Accounting Research
Vol. 8, N. 14, 2008, pp.1-22
ISSN: 1577-8517

Accounting for Collaborative Supply Chain Relationships: Issues and Strategies

Steve G. Sutton. University of Central Florida. USA/ University of Melbourne. Australia. Steve.Sutton@bus.ucf.edu

Georgia Smedley. University of Missouri- Kansas City. USA. smedleyg@umkc.edu

Vicky Arnold. University of Central Florida. USA/ University of Melbourne. Australia. Vicky.Arnold@bus.ucf.edu

Abstract. The purpose of this discussion paper is to explore the contemporary business model that has arisen with the advent of B2B e-commerce systems in order to better understand the improvements needed in the financial reporting model. The contemporary business model has relegated the enterprise-centric view of corporate competition and the current financial reporting model to insignificance in many instances. Rather, today's business environment is one dominated by competition between supply chains with an organization's success ultimately hinging on the viability and success of its supply chain partners as much as, or more than, enterprise-centric policies and decisions. As a result, these highly integrative systems connect supply chain partners in a manner that is more tightly coupled than most consolidated entities. Still, the current financial reporting model fails to even minimally capture the complexity of this new reality. This discussion paper provides the foundation for elaborating on a detailed discussion of how this business model could be more accurately captured through an enhanced business reporting model.

Key words: Object-oriented, financial reporting, information systems.

Submitted November 2007
Accepted January 2008

DOI: 10.4192/1577-8517-v8_1

1. INTRODUCTION

For over a decade, business consultants, and in turn corporate executives, have advocated the need for organizations to focus on their own core competencies and to leverage relationships with business and trading partners with a goal of improving efficiency of operations. The primary catalyst in this espoused business model has been the rapid integration and use of business-to-business (B2B) e-commerce to share information and to create viable value chain components across multiple tightly coupled organizations. B2B e-commerce technologies provide the electronic capability to link the operations of two or more organizations seamlessly in order to create an overall supply chain capable of acting as a single cohesive entity in the delivery of products to end customers. Such relationships create co-dependencies among partner organizations that result not only in the sharing of benefits through efficiency gains, but also a sharing of inevitable risks. From an enterprise risk management view, such risks can be particularly disconcerting as an organization generally has minimal control over the mitigation of risks at partner companies (Arnold *et al*. 2004).

In the process of automating connections with trading partners, organizations are increasingly dependent on upstream and downstream business partners to optimize production schedules and minimize inventories on hand. While organizations enter into this new business environment with the idea of maximizing efficiencies, they face significant business risks associated with the increased dependence on business partners to shorten cycle times and deliver materials and supplies on increasingly shorter notice. A further major source of unrecognized enterprise risks exudes not only from these tightly coupled supply chain relationships, but also from key outsourcers that perform vital functions in the overall value chain of the vast majority of organizations.

As these various business partners assume key responsibilities in organizations' value chains, individuals who invest in these organizations become increasingly under-informed as to the operations and business risks. The traditional business model assumes organizations compete in an essentially autonomous state where operations and risk can be assessed with an enterprise-centric view; unfortunately, this traditional model is rarely true in today's business environment. Rather, investors who use traditional financial reports to examine various organizations and make investment decisions are generally making such decisions

without a true picture of the viability and health of those organizations' value chain activities. An investor (or potential investor) examining the financial reports generated by an organization is rarely able to gain a true understanding of the risks facing that organization. Organizations do not provide the necessary information to understand whether critical business partners will be able to effectively implement new business processes necessary to implement process improvements. Absent such an understanding, the potential investor would be unable to assess the viability of the organization in terms of ability to adopt new technologies, refine business processes, and maintain competitiveness—opportunities dependent in part on business partners adaptability. In an era where Sarbanes-Oxley requirements are pushing organizations to implement effective enterprise risk management processes, organizations are increasingly recognizing that while they can outsource key business processes, they cannot outsource the risks from work stoppages and supply chain disruptions nor can they outsource the responsibility for controls over the information flowing across supply chains that ends up in the financial statements (Ernst & Young 2004). Yet, these financial statements fail to reflect these relationships and investors are largely left in the dark about the nature of relationships and related risks that organizations encounter in these tightly coupled partnerships.

The purpose of this paper is to elaborate upon the integrated nature of interorganizational relationships in the contemporary business model and to explore the issues that should be considered in the development of an external financial reporting model that adequately encompasses such relationships. This purpose is addressed in two stages. First, a review is provided on the evolving nature of business relationships from an enterprise-centric competitive model to a business environment where competition is better viewed as supply chain versus supply chain. Consideration is given to how this alternative view of the business environment affects the way in which enterprise risks should be assessed and the impact of these enterprise risks on the design of effective risk management programs. The second stage focuses on the issues that must be addressed in formulating financial reporting concepts that address enterprise risk across the supply chain in order to provide investors and other stakeholders with an understanding of the viability and security of the value chain. This discussion entails an examination of how to formulate the boundaries for measuring corporate viability from this broader interorganizational perspective and what dimensions

should be considered in formulating measures for reporting. Finally, some summary thoughts are provided to draw the concepts together and consider a future agenda for actions to enhance business reporting along the dimensions discussed herein.

2. EVOLVING NATURE OF BUSINESS RELATIONSHIPS

Over the past several years, organizations have utilized technology to link with other organizations to develop a very complex web of dependencies. These linkages have created a new set of risks not previously encountered in the business environment—interorganizational risk. Figure 1 illustrates how interorganizational risks fit into overall enterprise risk and the importance of the risks emanating from interorganizational dependencies. Interorganizational risks are created through alliances established with outsourcers and strategic business partners. The risks from these partnering relationships consist of three distinct levels: (1) business level risk, (2) application-user level risk, and (3) technical level risk. Each of these risks will be further discussed in the overall context of the changing business model from an organization competing with other organizations to a supply chain versus supply chain model.

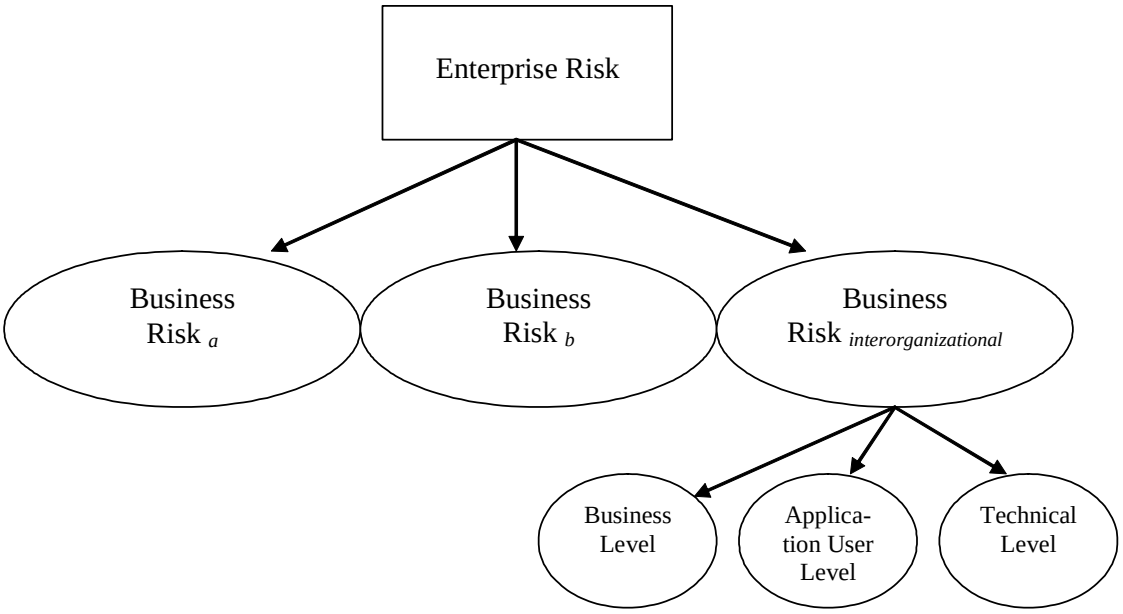

Figure 1.Risks Facing Organizations in an Extended Enterprise Environment

Supply Chain vs. Supply Chain Competition

Several factors have come together to transform the traditional, enterprise-centric model of survival to a model of interorganizational dependencies. The major factors include outsourcing core functions in the value chain, utilizing B2B e-commerce technologies to link with partner organizations, and aligning with strategic partners—a move that reduces the number of suppliers and vendors (and potentially customers) to a select few organizations that are willing to enter into partnering roles. This combination has drastically altered the competitive landscape. The traditional model of one enterprise competing against another enterprise for market share has evolved into an environment of competition between one enterprise's supply chain versus another enterprise's supply chain. Indeed, Dell Inc. and Wal-Mart Stores Inc. have become fixtures in strategic management courses and the popular business press for the manner in which they have dominated their competitors through reinvention of their supply chains (Papazoglu *et al.* 2000; Taylor 2003). Wal-Mart Stores Inc. and the Big Three U.S. Automakers (among others) have also become renown for requiring all suppliers to provide electronic data interchange (EDI) capability for the transfer of transaction data and electronic payment. The simplification of the B2B e-commerce environment with Internet-based web applications has made it even more feasible to push such models of integration. These companies all recognized very early the cost savings that arise from electronic processing of information and tight linkages between their information systems and their vendors' systems. (Arnold *et al.* 2004).

The evolution that such leading edge companies have driven in the marketplace have made partnering and outsourcing relationships key components of the value chain in contemporary business models with the primary focus on maintaining competitiveness. The results of a recent PricewaterhouseCoopers (PwC) CEO risk study indicate that CEOs as a whole are more likely than ever to outsource core business processes. These increases in outsourcing are driven primarily by desires to control cost, control the number of employees that must be managed, and to ensure quality through a competitive marketplace for service provision. The emphasis on outsourcing is not likely to be a short-term phenomenon given that 73 percent of the CEOs surveyed viewed the emphasis on outsourcing as long-term (PricewaterhouseCoopers 2004).

From a risk management perspective, a core problem in this urgent move to outsourcing and partnering relationships is that the vast majority of organizations have maintained an enterprise-centric view on systems issues while trying to execute an interorganizational view in their business models. Too often, each enterprise in the supply chain maintains its own systems and focuses on how to transfer certain key information items electronically between organizations. Only recently have organizations begun to share data from production planning systems in a fashion that allows other organizations in the supply chain to better control (and shrink) their inventory stocks. Additionally, sharing this information has become increasingly critical for an evolution to a complete just-in-time mode across the supply chain. Without reliable information regarding the information processing capabilities and security of partner enterprises' internal (business information processing) and external (e-commerce integration systems) information systems, a given enterprise has little understanding of the true level of risk it absorbs as a component of a given supply chain competing for market share (Sutton and Hampton 2003).

For those who might question the impact of supply chain partners on an organization's overall operations, many documented examples demonstrate significant impact due to partner failure. Two of the more publicized failures were Nike and Cisco Systems. Nike's crisis came in May 2001 when reported sales for the prior quarter had to be reduced by $100 million because of confusion in its supply chain. Cisco Systems experienced an even bigger hit when $2.2 billion was written off for unusable inventory resulting from problems in the supply chain. The financial statement impact is only a small part of the story if one also considers that Nike's stock dropped 20 percent in value after its announcement. Studies show that a stock value drop of 7.5 percent upon announcement of supply chain interruptions is average and a drop of 18.5 percent is typical over the 12 month period following the announcement (Taylor 2003).

The failure to assure reliability across the information supply chain, as in the Nike and Cisco Systems examples, is only part of the problem. The greater risk for most enterprises is the potential for disruptions in the supply chain that may force extended shutdowns of operations. Many enterprises have resorted to insurance to try to fund such a potential disruption, but only smaller companies try to insure the entire potential impact while larger organizations are more prone to accept a

portion of the risk internally (Taub 2002). While insurance may help organizations weather the disruption, the impact on stock price resulting from such a disruption is unlikely to be offset by insurance. In the meantime, the insurance company may also be unable to meet its obligations if the costs are significant, or even more likely, may try to avoid liability by rejecting the occurrence as an insured event. The result could be lengthy lawsuits that increase the likelihood a company goes out of business before ever collecting. Curiously, for organizations not purchasing insurance against disruptions, the potential liability and risk is rarely if ever reported and to the authors' knowledge never questioned by the auditor.

The potentially high risk nature of aligning with a selective set of partners across a supply chain makes the selection and/or integration of business partners even more critical as enterprises implement a variety of strategies for reducing business cycle time including vendor managed inventory (VMI), just-in-time (JIT) manufacturing, and quick response retailing (QR). Organizations need to place great importance on selecting and retaining quality business partners to ensure stability (Khazanchi and Sutton 2001; Greiger 2003). An enterprise should consider the capabilities a given partner has to integrate technologies that will support integrated business processes and communication with information systems of all partners across the supply chain. The integration process can be painful, and the expense and complexity of making such linkages will frequently secure business partner relationships and provide strong motivation to maintain stability among the various members in the supply chain (Grover *et al*. 2002; Shin and Leem 2002).

For an investor, little information is available by which to understand and assess the viability of such trading partner relationships. The enterprise-centric nature of the financial reporting model was designed to provide a broad view of organizations in a different era. In the contemporary business environment the financial reporting model is insufficient for an investor to attain a good, broad view of today's organization. As discussed in the subsequent section, this broader view of organizations is critical to understanding key business risks facing a potential investee.

Understanding Interorganizational Business Risk

The rapid and widespread adoption of B2B e-commerce has been well-documented in the business press over the past five years. Indeed, in 2003 as the requirements for strong internal controls as mandated in the Sarbanes-Oxley Act captured much of the attention in IT budget, e-business expenditures still rivaled security expenditures for the largest share of IT budgets. In many respects, e-commerce and security expenditures served to work hand-in-hand as companies took steps to improve security as a means of providing business partners peace of mind (Ware 2002). As some of the euphoria behind e-commerce began to fade with the demise of e-commerce company stocks, the realization set in for CIOs that implementing basic B2B e-commerce systems were unlikely to have more than a marginal benefit at best. The reality is that EDI has enabled interorganizational systems for some 30 years, and most enterprises have had some level of EDI integration in place for many years. However, such integration of transaction-level systems generally falls far short of a real collaborative relationship. Research shows that the major benefits from B2B relationships at this point in time come primarily from collaboration—not integration (Lee *et al.* 2003).

Unfortunately, in many cases an organization's business partners simply are not prepared to operate in a collaborative B2B e-commerce environment—usually because of limitations in either technical, personnel or security capabilities. Several large retailers and manufacturers have, in the past, required vendors and suppliers to adopt EDI or some other form of B2B e-commerce. Research suggests such a strategy is not without risks. Forcing vendors and suppliers to implement B2B e-commerce capability often leads to distrust and can inhibit voluntary use of B2B applications beyond what is absolutely required (Hart and Saunders 1997). In other cases, relationships often degenerate into conflict situations that result in worse rather than better collaboration (Hart and Saunders 1997; Kumar and vanDissel 1996). Regardless, a current business environment that feeds competition between supply chains in an industry dictates that to sustain competitiveness, B2B integration is imperative and a greater focus should be placed on assisting business partners in the integration of new technologies. If current partners cannot be brought along technically or simply refuse to make appropriate efforts to facilitate collaboration, an organization may well need to step back and assess alternative business partners' capability and willingness to engage in effective B2B integration

that will achieve a desired level of collaboration (Angeles and Ravinder 2000; Khazanchi and Sutton 2001; Kurnia and Johnston 2000). In today's Internet world there are many potential vendors available that do have the capabilities to participate.

Failure to effectively integrate policies for trading partners and to secure information across the supply chain can heighten a number of risks for an organization. First, care should be taken as to what information is shared with a trading partner through B2B e-commerce collaboration tools; and policies that govern the trading partner's use of that information should be implemented. Information accessibility beyond that which is needed may provide a trading partner with information that gives the partner a competitive edge in subsequent negotiations. Alternatively, an organization would be at risk if a third-party hacked into a trading partner's system, and then gained access to their system by using the trading partners' authorized accessibility. There is also the risk that viruses and worms that have infected a trading partner's systems could be passed to an organization's systems through the access established to support interorganizational communications and information sharing. Standards need to be in place on both ends of a trading relationship that clearly articulate the policies and procedures that should be implemented to assure adequate protection of systems—including such standard items as mandating maintenance of up-to-date antivirus software.

Most investors and stockholders likely assume that such policies are followed and enforced, but experience tells a different story. One anonymous security manager discusses the adventures experienced when integrating a newly acquired company's systems with their secure systems. Simple controls such as data backups were poorly executed. While there were good controls in other areas such as the security over databases, there were poor controls over the data being entered into the databases. In another situation, an information technology (IT) worker who preferred to work at home had set up a direct DSL line into the his organization's computer systems. This allowed the worker to by-pass the virtual private network (VPN) normally required of employees for home connection. The IT worker with the DSL line then set up an unsecured home wireless network which resulted in anyone in the neighborhood having wireless access to the corporate systems—and through those systems an unauthorized link into the acquiring company's systems

(Thurman 2004). These are only a couple of simple examples of how seemingly innocuous actions result in a major breach of security. Maintaining security in such interorganizational systems environments becomes very difficult when an organization has little control over the actions of a trading partner and little knowledge of the actual security policies and procedures that are enforced on an on-going basis.

The net effect is that enterprises face a dual-edged sword. On one side, they face the inevitable consequences of failing competitiveness if effective B2B e-commerce systems supporting collaborative supply chains are not implemented. On the other side, they face the escalated risks of exposing their information systems to business partners' systems that may not contain adequate levels of technology integration or security. Investors face the issue that they know little about a company's trading partners and even less about the policies and procedures that are in place to minimize the enterprise risk being absorbed in such relationships.

Extended Enterprise Risk Management

Organization's enterprise risk management efforts coupled with the risk assessment demands of the U.S. Sarbanes-Oxley Act leave many organizations in a position of needing to establish processes to identify and monitor risks in B2B e-commerce-driven relationships. While most large organizations are well into their reporting for Section 404, an evolving view of these mandates is that expectations will continue to shift over the coming years. Most organizations are arguably still deficient in terms of assessing and controlling for risk environments that extend beyond their organizational boundaries. Yet, in order to truly have enterprise risk management processes in place as mandated by these regulations, most organizations must greatly increase the scope of such processes. Likewise, that broader vision of enterprise risk management needs to be communicated to investors who currently lack such information in assessing potential investments.

The first official position taken with a direct link to B2B e-commerce risks was actually put forth by the International Federation of Accountants (IFAC) via *International Audit Practice Statement 1013* (2002). The practice statement identifies three aspects of B2B e-commerce relationships that should be considered and assessed: (1) IT business processes, (2) IT applications, and (3) IT infrastructure. Audit practice statements are limited to putting forth only

recommended guidelines for audit processes that should be applied. These categories are very similar to those that have emerged in the research literature as a foundation for B2B e-commerce assurance. The Khazanchi and Sutton (2001) framework for B2B e-commerce risk assessment consists of three equivalent aspects: (1) business level risk, (2) application-user level risk, and (3) technical level risk.

Business level failures can leave trading partners with poorly integrated business processes, inefficient production models, and an inability to react in a timely manner necessary for the effectiveness and viability of the overall supply chain. Failures at the application level can result in instability of applications fundamental to the support of trading partners' systems effectiveness, can impede timely delivery of product across the supply chain, and can force supply chain partners to absorb increased safety stock costs and potential production interruptions while awaiting materials from suppliers. Failures at the technical level may result in missing orders, data theft by corporate spies, and corruption of data and systems as a result of viruses and worms infiltrating through on-line connections.

All three levels of risks need to be carefully assessed and monitored to effectively manage enterprise risk—even though such risks exist due to externalities. These three levels of risk have the ability to individually and/or jointly disrupt supply chains and accordingly impact all organizations across the supply chain. Effective enterprise risk management is only possible when an extended-enterprise view is adopted in the formulation of risk management efforts.

3. ISSUES IN REPORTING ON COLLABORATIVE RELATIONSHIPS

As noted throughout this discussion, these concerns over risks are not only a corporate management issue, but also an investor issue. Filers of 10-K annual reports with the U.S. Securities and Exchange Commission (SEC) are required to document key business data and business risks. However, rarely do such business and risk discussions provide even minimal information about dependencies in such interorganizational relationships. While the importance of such relationships was highlighted in the recent bankruptcy filing of Delphi, an automotive systems manufacturer that is a key supplier and partner of General Motors in the U.S., even

relationships with smaller vendors can be critical to operations. The real challenge is in deciding who and what should be analyzed in reports for investors and other stakeholders—and, of course, then how to get companies to actually provide such reports.

Scoping the Boundaries for Reporting

Much could be learned by accounting standards setters from a look at adopted views of management. Management research has long considered some of the most vital members of an organization to be the 'boundary spanners'—the managers in the organization that move back and forth freely between partnering organizations, making relationships work and building trust (Rieple *et al.* 2005). The financial reporting model, however, focuses on an enterprise-centric view of an organization which is that part of the organization wholly within the legal definition of the organization, essentially ignoring the areas at the boundaries where organizational success is heavily dependent on transcending those boundaries and establishing tightly coupled partnering relationships.

This is not the first time the reporting model has faced limitations in information content due to tightly coupled organizations—but the key in the past has been that an organization takes over a partner and integrates them into the company ownership. Still, arguably much could be learned now on setting the boundaries for interorganizational relationships by reviewing the manner in which the issue was tackled in an era of mergers and acquisitions. The 1960's saw a tremendous increase in mergers and acquisitions that translated into a need, on the part of financial analysts, for increased information concerning segment reporting. The initial response from the Accounting Principles Board, the New York Stock Exchange, the Federal Trade Commission, and the SEC was to urge voluntary disclosure of industry, export sales, and domestic and foreign operations. The big corporations that were involved in the mergers and acquisitions, however, were resistant to such disclosures due to their alleged concerns of disclosing competitive advantages in the process of disclosing segment information. In 1969 the SEC required a report on segment line information for registration purposes. Companies with material functional segment income opposed this SEC requirement, and ensuing legal battles extended to the Supreme Court (see APB Statement No. 2, SEC Rule 303(e), and Pacter (1993)).

In 1976 the Financial Accounting Standards Board (FASB) released FAS 14, Financial Reporting for Segments of a Business Enterprise. This standard called for disaggregated financial accounting information for the following aspects of a company's operations when such disaggregation was deemed to be material to external users of financial information:

1. A company was required to disclose revenues, operating profit/loss, identifiable assets, aggregated depreciation, capital expenditures, and equity in net income by industry segments.
2. A company was required to disclose revenues, operating profit/loss, and identifiable assets for the operations of each significant foreign geographical area.
3. A company had to report the amount of revenues derived from exported products from domestic operations to unaffiliated customers in foreign markets.
4. A company was required to disclose the amount of revenue derived from sales to each major customer. The existence, though not the name, of each qualifying major customer and the associated revenues had to be disclosed.

Materiality was to be determined on the basis of any one of three quantitative thresholds: revenue tests, profit or loss tests, or asset tests.

In 1997 the FASB released FAS 131 Disclosures about Segments of an Enterprise and Related Information. In part, FAS 131 responded to growing complaints from the Association for Investment Management and Research (AIMR) that FAS 14 did not adequately require needed disclosures. The AIMR argued that management too often manipulated information about segments' revenues, profits (losses) or assets in order to avoid disclosing information about those segments. FAS 131 replaced many parts of FAS 14, provided a guiding set of objectives for segment reporting, and required that the "management approach" for determining which segments be disaggregated in a company's financial statements. The objectives of segment reporting, according to FAS 131, are to provide information about business activities so users of financial information may:

- better understand the company's performance
- better assess the company's prospects for future cash flows

- make more informed decisions about the company as a whole

The management approach requires a disaggregation of segment information if management disaggregates that segment for operating decision purposes.

The release of FAS 14 spurred a great deal of research. The results of this research have been well documented by Pacter (1993), and center, primarily, on the market effects of disaggregated financial information along the lines of industry segments, geographical segments, and export sales. Research involving the "major customer" aspect of FAS 14 has been limited primarily to reporting practices (see Beresford and Buckner, 1978; Steele, 1983; and Thompson and Fowler, 1993). Since the release of FAS 131, research has focused primarily on market changes from FAS 14 to FAS 131 (see Tang and Zhao, 1999; Street *et. al.*, 2000; Botosan and Stanford, 2005; Ettredge et. al., 2006; and Journal of Accountancy, 2006) and on the international implications of FAS 131 (see Wallace, 2000; Accountancy, 2006; and Wendell, 2006). The sole study found to focus on major customers (Gosman, *et. al.*, 2004) examined the profitability of firms that were identified as major customers by companies required to disaggregate such information. Findings suggest that investors both recognize the value of such information and place higher value on the major customer companies.

The dearth of investigation into the market effects of information disaggregated to include major customers belies the importance of the information disclosure. An examination of data reported in Accounting Trends and Techniques from 1979 to 2003 shows that of the 600 firms analyzed over this period, the number of firms reporting sales to major customers rose from 85 to 178—a trend indicative of the move towards partnering type relationships between specific suppliers and specific customers. However, such reporting requirements assume that revenue (e.g. focus on customers) is the primary disclosure of interest. This ignores the important role that suppliers and outsourcers might have on an enterprise's viability and overall risks. In the contemporary environment, it seems imperative that the FASB (and the IASB) consider how these rules for ownership and customers might in parallel be adopted for integrating the impact from strategic trading partners—both upstream and downstream in the supply chain. As Vasarhelyi and Alles (2007) highlight within their Galileo Disclosure Model, this concern has existed for some time and is also a key component of the Jenkins Committee recommendations that remain unaddressed by the FASB or the IASB.

What constitutes a material supplier? What constitutes a material outsourcer? What information from these relationships should be disclosed to meet various stakeholders' needs? This latter question relates to the measurement issues and is where this discussion is redirected at this point.

Establishing Measurement Criteria

Establishing the criteria that should be used to measure a given dimension of an organization's financial position is rarely a simple feat. First, one needs to understand what information would be important to what stakeholders under what conditions for what purpose. Second, once the need is better articulated, developing consistent measures that are useful across the range of organizations is challenging and may be elusive.

If one considers the dimensions that are currently reported by organizations, one area seems glaringly important. The required disclosures in the annual report related to Business Data and Business Risks should include risks associated with dependencies across the supply chain both upstream and downstream. While provisions exist as noted, for basic information related to major customers, other information on trading partner relationships is minimal if existent at all within most organization's annual report disclosures. Yet, as highlighted in the first parts of this discussion paper, the risks are high and often uncontrolled in contemporary interorganizational relationships.

- Little is known about the security of organizations B2B e-business operations and the viability of partners B2B operations.
- How well prepared are organizations to continue to streamline operations and reduce cycle times?
- How prepared are organizations to adopt flexible approaches that maintain agility and allow them to quickly adapt to changes in the marketplace?
- Most importantly from the perspective of the discussion here, how prepared are organizations trading partners to facilitate the streamlining and adaptation of an organization to meet market needs?

Absent better disclosures, investors and other stakeholders will essentially continue to gamble that organizations are monitoring and controlling such risks, such that those organizations will remain competitive in the marketplace.

The challenge is to figure out what should be measured. For instance, research has shown that reports of Internet downtime for web-based companies due to hacker attacks cause negative fluctuations in stock prices (Richardson and Ettredge 2003). Would investors benefit from having a priori information as to how companies are protecting themselves from denial of service attacks as well as other types of sabotage to e-business systems? More research is needed to understand how such information might facilitate investors' decision making. The key is that a known effect is present.

Similarly, research has shown that investments in IT experience and e-commerce technologies result in positive reactions from investors (Chatterjee *et al.* 2001; Guan *et al.* 2006; Dehning *et al*. 2006). Of particular note is the Dehning *et al.* (2006) study that demonstrates positive performance effects from the use of IT-based supply chain management systems within the manufacturing sector. The study shows the positive effects of interorganizational systems, while the presence of supply chain management systems technologies would not easily be detected within an organization's annual report as even necessarily existing. Again, investors and other stakeholders are disadvantaged by inadequate disclosures.

Research has also focused specifically on the B2B e-commerce aspect of collaborative relationships with a focus on the key components of risk (Arnold *et al*. 2006). One would assume that many of the risks would be covered by adequate internal controls as reported upon in management's and the auditor's reports on internal controls. However, organization's management and their auditors have been inconsistent in their expectations of control coverage extending to trading partners. Most appear to be requiring SAS 70 reports on the internal control coverage of a third-party, while some are requiring additional procedures beyond that covered under a standard SAS 70. The internal control reports have exposed some of the issues that are present. For instance consider Iomega's Annual Report for 2004 where a trading partner produced a SAS 70 report with three internal control deficiencies two weeks before the filing of Iomega's report. The deficiencies were identified as:

"(i) pervasive control weaknesses in the third-party distribution/logistics service provider's general information technology ("IT") controls relating to change management and system access and (ii) control weaknesses in the third-party distribution/logistics service provider's inventory management processes, primarily in the areas of physical security and inventory receipts, combined with (iii) a lack of adequate or comprehensive compensating internal controls at the Company." (Iomega 2005, p. 3)

Yet, absent reporting that occurs through default via the internal control report, investors and other stakeholders fail to get vital information related to these relationships.

Sutton *et al.* (2008) look beyond just factors that would fall under the guise of internal controls. Rather, many of the factors deal with more strategic level linkages and the impact on business processes. The risk factors are identified across three levels: technical level, application-user level, and business level. Technical level factors that in most likelihood go beyond simply internal control reporting include risks related to trading partner's competency in e-commerce technologies and applications, capacity, resiliency, adherence with regulatory requirements, migration capability to new platforms, and the flexibility and scalability of systems. Application-user level factors falling outside the typical internal control scope include emphasis on integration of B2B linkages with internal processes, sustainability of e-commerce marketplace, and simply the trust in the trading partner. Business level factors are rarely covered under the internal control scope and would include risks such as trading partner's understanding of their own business processes, understanding of associated risks with non-compliance with regulations and laws, effectiveness of project management, strategic focus on IT integration, and the ability to protect a distinguished brand in an e-commerce environment. Effective risk management in these areas is critical, yet for an outside investor, visible evidence of such risk management is limited at best.

As a greater understanding of the risks surrounding interorganizational relationships is garnered, it is critical that consideration is given to how risk mitigation efforts can be effectively communicated to investors and other stakeholders. The current reporting system is simply insufficient to address these issues, yet at this point we have little in the way of meaningful measures or metrics

that can be applied and communicated to users of financial reports. In the current interorganizational environment, a better understanding of these relationships is critical to maintaining the usefulness of financial reports to investors and other stakeholders within certain industry sectors.

4. CONCLUDING PERSPECTIVES

The purpose of this discussion paper has been to more clearly articulate the issues surrounding interorganizational relationships across supply chains, and the need for investors and other stakeholders that use financial reports to have access to enhanced business reporting related to such relationships. These relationships are complex and, in many situations, create co-dependencies among organizations. While legally they remain separate entities, the reality is that today's integrative supply chains are more representative of the consolidated enterprises of the 1970s where companies focused on complete ownership across both vertical and horizontal business process components. Now in an era where the focus is on core competencies and developing business partner relationships to handle all other critical processes to an organizations value chain, the simple fact that a legal ownership connection does not exist is not indicative that the partnering entities are in any way independent. Rather the co-dependencies may in reality be of more potential concern to investors than the legally related consolidated corporations that do report as combined entities.

Our financial reporting model was developed within the context of a much more simplistic business environment and is not necessarily well suited to the complexities inherent today. Technology has allowed new business forms to emerge, yet accounting which considers itself the core information flow of organizations has failed to maintain its usefulness as these new business forms have arisen. The need for the development of an enhanced business reporting model grows every day. It is imperative that the research community embrace this need for change and accordingly assess how new research efforts can be more proactive and leadership oriented as opposed to the largely *ex post*, descriptive posture that dominates our contemporary academic community.

5. REFERENCES

AICPA (1983): *Accounting Trends and Techniques*. American Institute of Certified Public Accountants. New Jersey.

AICPA (1993): *Accounting Trends and Techniques*. American Institute of Certified Public Accountants. New Jersey.

AICPA (2005): *Accounting Trends and Techniques*. American Institute of Certified Public Accountants. New Jersey.

ANGELES, R.; RAVINDER, N. (2000): "An empirical study of edi trading partner selection criteria in customer-supplier relationships", *Information & Management* vol. 37: 241-255.

ANONYMOUS (2006): "Financial reporting: International briefing: IASB", *Accountancy*, March: 102.

ANONYMOUS (2006): "Understanding the entity and its environment and assessing the risks of materiality", *Journal of Accountancy,* May: 129.

ARNOLD, V.; HAMPTON, C.; KHAZANCHI, D.; SUTTON, S.G. (2004): *Enterprise Risk Management: Identifying Risks in B2B E-Commerce Relationships (w/)*. Institute of Internal Auditors Research Foundation. Altamonte Springs, Florida.

BERESFORD, D.R.; BUCKNER, C.O. (1978): "Segment Reporting Practices", *The CPA Journal*, December: 37.

BOTOSAN, C.A.; STANFORD, M. (2005): "Managers' motives to withhold segment disclosures and the effect of SFAS No. 131 on analysts' information environment", *The Accounting Review*, July: 751-771.

CHATTERJEE, D.; RICHARDSON, V.; ZMUD, R. W. (2001): "Examining the shareholder wealth effects of newly created cio positions", *MIS Quarterly*, vol. 25, n. 1.

DEHNING, B., RICHARDSON, V.; ZMUD, R.W. (2006): "The financial performance effects of IT-based supply chain management systems in manufacturing firms", *Journal of Operations Management* (forthcoming).

ERNST & YOUNG (2004): *Emerging Trends in Internal Controls: Initial Survey* . Ernst & Young. http://www.ey.com.

ETTREDGE, M.L.; KWON, S.Y.; SMITH, D.B.; STONE, M.S. (2006): "The effect of STAS No. 131 on the cross-segment variability of profits reported by multiple segment firms", *Review of Accounting Studies*, March: 91.

GOSMAN, M.; KELLY, T.; OLSSON, P.; WARFIELD, T. (2004): "The profitability and pricing of major customers", *Review of Accounting Studies*, March: 117-139.

GREIGER, M. (2003): "Electronic marketplaces: a literature review and a call for supply chain management research", *European Journal of Operational Research*, vol. 144.

GROVER, V.; TENG, J.T.C.; FIEDLER, K.D. (2002): "Investigating the role of information technology in building buyer-supplier relationships", *Journal of the Association for Information Systems*, vol. 3.

GUAN, L.; SUTTON, S.G.; CHANG, J.; ARNOLD, V. (2007): "Further Evidence on Shareholder Wealth Effects for Announcements of Newly Created CIO Positions", *DATABASE of Advances in Information Systems* (forthcoming).

HART, P.J.; SAUNDERS, C.S. (1997): "Power and trust: critical factors in the adoption and use of electronic data interchange", *Organization Science*, vol. 8, n.1: 23-42.

IFAC (2002): *International Audit Practice Statement 1013*. International Federation of Accountants.

KHAZANCHI, D.; SUTTON, S.G. (2001): "Electronic commerce assurance services: a framework and implications", *Journal of the Association for Information Systems*, January.

KUMAR, K.; VAN DISSEL, H.G. (1996): "Sustainable collaboration: managing conflict and cooperation in interorganizational systems", *MIS Quarterly*, September: 279-300.

KURNIA, S.; JOHNSTON, R.B. (2000): "The need for a processual view of inter-organizational systems adoption", *Journal of Strategic Information Systems*, vol. 9: 295-319.

LEE, S.C.; PAK, B.Y.; LEE, H.G. (2003): "Business value of B2B electronic commerce: the critical role of inter-firm collaboration", *Electronic Commerce Research and Applications*, vol. 1.

PACTER, P. (1993): *Reporting Disaggregated Information*. Financial Accounting Standards Board. Norwalk, CT.

PAPAZOGLOU, M.P.; RIBBERS, P.; TSALGATIDOU, A. (2000): "Integrated value chains and their implications from a business and technology standpoint", *Decision Support Systems*, vol. 29.

PRICEWATERHOUSECOOPERS (2004): *Managing Risk: An Assessment of CEO Preparedness*. PricewaterhouseCoopers. http://www.pwc.com.

RICHARDSON, V.; ETTREDGE, M. (2003): "Information transfer among internet firms: the case of hacker attacks", *Journal of Information Systems*, Fall.

RIEPLE, A.,.; HABERBERG, A.; GANDER, J. (2005): "Hybrid organizations as a strategy for supporting new product development", *Design Management Review*, vol. 16, n. 1.

SHIN, K.; LEEM, C.S.: (2002): "A reference system for internet based inter-enterprise electronic commerce", *The Journal of Systems and Software*, vol. 60.

STEELE, L.F. (1983): "Disclosure of segment information – SFAS #14", *The CPA Journal*, October: 34.

STREET, D.L.; NICHOLS, N.B.; GRAY, S.J. (2000): "Segment disclosures under SFAS No. 131: Has business segment reporting improved?", *Accounting Horizons*, September: 259-285.

SUTTON, S.G.; HAMPTON, C. (2003): "Risk assessment in an extended enterprise environment: re-defining the audit model", *International Journal of Accounting Information Systems*, vol. 4, n. 1.

SUTTON, S.G.; KHAZANCHI, D; HAMPTON, C.; ARNOLD, V. (2008): "Risk analysis in extended enterprise environments: identification of critical risk factors in B2B e-commerce relationships", *Journal of the Association for Information Systems* (forthcoming).

TANG, R.Y.W.; ZHAO, J. (1999): "A look at the segment reporting practices of some Fortune 500 Companies", *The Journal of Corporate Accounting and Finance*, Spring: 10-12.

TAUB, S. (2002): "Companies not prepared for interruptions, say CFOs", *CFO* , April: 22.

TAYLOR, D.A. (2003): "Supply chain vs. supply chain", *Computerworld*, November: 10.

THOMPSON, J.H.; FOWLER, K.J. (1993): "Quantitative guidelines: Guidance based on professional pronouncements", *The CPA Journal*, March: 48.

THURMAN, M. (2004): "Security managers journal: overwhelmed by Sarbanes-Oxley", *Computerworld*, March: 1.

VASARHELYI, M.A.; ALLES, M. (2007): *The Galileo Disclosure Model (GDM): reengineering Business Reporting through using new technology and a demand driven process perspective to radically transform the reporting environment for the 21st century*. Working paper, Rutgers Accounting Research Center.

WALLACE, W.A. (2000): "Action needed to align reporting requirements", *Accounting Today*, vol. 14, n. 21: 14-16.

WARE, L.C. (2002): "Security and e-business will dominate 2003 it spending", *Computerworld*, December: 2.

WENDELL, P.J. "IASB proposals on segment reporting and interim financials", *SEC Accounting Report*, March: 8.

.