

A b s t r a c t

Despite high expectations, transactions through Internet based electronic marketplaces have not expanded rapidly. Recent evidence suggests that the peculiar characteristics of purchasing through Internet-based electronic marketplaces may actually increase sourcing risk. Such marketplaces may expose buyers to suppliers with whom they have no transaction history. Transacting through a public medium (Internet) may raise security and privacy concerns. Along with an evolving legal framework for governing online transactions such concerns may add to the overall cost of transactions. This paper by drawing on transaction cost economics, agency theory, resource dependence theory and channel risk literature identifies transaction risk, security risk and privacy risk as three dimensions of sourcing risk that buyers may face in transacting through Internet-based electronic marketplaces. It also proposes a risk-control framework that captures the linkage between sourcing risk and control systems. This linkage expounds on various control systems that may mitigate sourcing risk facing the buyers and make Internet-based electronic marketplaces conducive to conducting transactions. The proposed framework can assist market operators in developing effective control strategies that minimize sourcing risk and bolster participation.

Keywords: electronic markets, sourcing risk, control systems, transaction process

A u t h o r s

Khawaja A Saeed

(khawaja@sc.edu) is a doctoral candidate in the management science department at the University of South Carolina. He has an M.B.A. in Technology Management from Asian Institute of Technology in Thailand. His areas of research interest are electronic commerce, inter-organizational systems, supply chain management, and information technology use. His work has appeared or is forthcoming in *CACM*, *Information Systems Journal*,

Controlling Sourcing Risk in Electronic Marketplaces

KHAWAJA A. SAEED AND ROBERT A. LEITCH

International Journal of Electronic Commerce, and *Journal of End User Computing*.

Robert A Leitch

(leitch@moore.sc.edu) is a Professor of Accounting and the Wilbur S. Smith Distinguished Foundation Fellow at the University of South Carolina Moore School of Business. He has co-authored two books in accounting information systems and in management information systems. His research interests include information system development, cost management systems, analytical review procedures, and statistical sampling. He has published articles in various journal including *Management Science*, *Journal of the American Statistical Association*, *Biometrika*, *Decision Sciences*, *Journal of Financial and Quantitative Analysis*, *The Accounting Review*, *Journal of Accounting Research*, *Auditing: A Journal of Practice and Theory*, *Journal of Management Accounting Research*, *Journal of Information Systems*, *Journal of Accounting Literature*, and *Management Accounting Research*.

INTRODUCTION

The emergence of the Internet as a viable channel for exchange activity, especially among firms, has generated immense interest in both research and practitioner communities. Companies such as Cisco, DELL, GE and IBM have reaped cost savings and process efficiencies through Internet-based procurement. Consequently, there has been a surge in the number of electronic marketplaces that facilitate exchange activity among buyers and suppliers through the Internet. ChemConnect.com, Assetsmart.com and SciQuest.com are examples of such electronic marketplaces. Despite high expectation of success, the adoption and use of such marketplaces has not taken off as expected (Sklar 2001). Thus, it is important to understand how Internet-based electronic marketplaces can boost participation, which is central to their success.

Anecdotal evidence suggests that buyers are wary of transacting business with suppliers over the Internet via electronic marketplaces. Lack of security, organizational/legal issues, and exposure to suppliers with whom buyers have not transacted before are suggested as the main barriers to online transactions among organizations (Archer and Gebauer 2002; Schoder and Yin



2000). These issues contribute towards increasing sourcing risk associated with conducting transactions through Internet-based electronic marketplaces. Electronic intermediaries have proactively employed different control systems under the rhetoric of assurance and trust based services to make electronic marketplaces more conducive to conducting transactions. However, previous research has not explicitly addressed the linkage between sourcing risk and control systems in an electronic marketplace context. Limited guidance exists on what control systems may be appropriate in mitigating different types of sourcing risk. This paper intends to explore this linkage. It presents a framework that expounds on types of sourcing risk and corresponding control systems that help alleviate these risks. Such a framework can assist electronic intermediaries in developing control systems to make the trading environment more conducive to exchange activity and can be instrumental in the success of their business models.

Exchange of goods and services among organizations or individuals is a fundamental economic activity. Transaction cost economics, resource dependence theory, and to some extent agency theory, have all been employed to predict the appropriate exchange design. These perspectives argue that the main problem related to exchange activity is the behavioural uncertainty of the transacting parties and propose control systems that try to minimize uncertainty (Stump and Heide 1996). Research on channel risk proposes that the channels through which a product is purchased pose different levels of sourcing risk to the buyers (McCorkle 1990). Researchers have found that a buyer's risk perception is higher when a product is purchased from a direct channel rather than from a store (Grazioli and Jarvenpaa 2000). Previous research provides insights into various sources of risks that buyers may face while purchasing a product. Some risks are specific to purchasing from electronic channels, while others are independent of the medium used for conducting the transaction.

At a broad level, sourcing risk within the context of this study is defined as a buyer's perception of risk and adverse consequences of engaging in a transaction

through an Internet-based electronic marketplace (Dowing and Staelin 1994). Review of the literature shows that channel risk (McCorkle 1990), opportunism risk (Williamson 1979), adverse selection risk (Bergen *et al.* 1992), operations risk (Clemons *et al.* 1993), authentication risk, and security risk (Kumar and van Dissel 1996) are different types of sourcing risk that may exist in the context of procurement activity. The peculiar nature of purchasing from an Internet-based electronic marketplace may elevate these risks. For example: the buyer's lack of ability to observe the seller's behaviour directly; disparate legal frameworks; concerns regarding security of the trading platform; and apprehension about handling of purchasing data by a third party (market operator) are issues that can significantly increase sourcing risk.

An important aspect of sourcing risk is its relation to transaction costs. Clemons *et al.* (1993) propose that risk is another form of cost (Table 1). Thus, an increase in sourcing risk actually inflates the overall transaction cost and may make procurement from an electronic marketplace less desirable. Increased sourcing risk related to a transaction, may also reduce many of the search-related benefits associated with using electronic marketplaces (Bakos 1991). In order to induce buyers to conduct transactions, it is important to investigate what options do Internet-based electronic marketplaces have in mitigating sourcing risk.

Previous studies have highlighted a range of control systems such as qualification procedures (Heide and John 1990), credible commitments (Anderson and Weitz 1992), and monitoring (Lal 1990) for managing risk associated with exchange activity. Research on electronic intermediaries suggests that technical instruments (i.e. security and privacy tools), screening procedures for vendors and customers, and online access to information may act as control options (Archer and Gebauer 2002). Assurance and trust-based services are control options intended to build impersonal trust that is created by institutional or structural arrangements in contrast to familiarity trust arising from repeated interactions (Pavlou 2002). Control systems that promote impersonal

Table 1. Transaction costs and sourcing risk

| Source of transaction costs | Cost perspective | Risk perspective |
|---|---|-----------------------------------|
| Coordination costs | Screening and selection costs | Adverse selection risk |
| | Communication and negotiation costs | Contract/ legal risk |
| | Contracting costs | Repudiation risk |
| | Measurement costs | Post contractual performance risk |
| Opportunity costs (Transaction risk) | Failure to identify the appropriate partners | Post contractual conflict risk |
| | Productivity losses through effort adjustment | Opportunism risk/Moral hazard |
| | | Adverse selection risk |

Note: Cost perspective adapted from Rindfleisch and Heide (1997).

trust may make the trading environment more conducive to conducting transactions and facilitate higher level of participation (Pavlou 2002). Effective control systems that mitigate sourcing risk may be an important factor in adoption and use of electronic marketplaces (Lee and Clark 1997).

This study aims to frame the linkage between sourcing risk and control systems by integrating previous research. We develop a risk-control framework for electronic marketplace procurement activities. This framework can be used systematically to identify the sourcing risk a company is exposed to while transacting through electronic marketplaces. By assessing effectiveness of control systems and their interdependence this study can help companies in developing control strategies to mitigate sourcing risk. By providing an initial discussion on these issues, this study also attempts to stimulate future research in this domain.

LITERATURE REVIEW

Literature on understanding the exchange phenomenon in the context of electronic channels is in a nascent stage. However, research on governance structure and channel risk can be extended to evaluate sourcing through Internet-based electronic marketplaces (Sarkar *et al.* 1996). The approach that we follow is to first elaborate on the notion of electronic marketplaces and assess issues that are peculiar to procurement from the Internet. Then, we examine how these issues can be viewed through different research perspectives. This allows us to pose some interesting questions that are subsequently addressed by the research framework.

Bakos (1991) defines an electronic market as an inter-organizational system that allows the participating buyers and sellers to exchange information about prices and product offerings. A market has also been defined in terms of its functions. Bakos (1998) posits that markets (electronic or otherwise) perform three functions: (i) they match buyers and sellers; (ii) facilitate exchange of information, goods, services, and payments associated with market transactions; and (iii) provide an institutional infrastructure, (i.e. legal and regulatory framework) that enables efficient functioning of the market.

Researchers argue that the main advantages of using electronic marketplaces are reduced search costs and lower prices for buyers, making sourcing through market mechanisms more cost efficient (Choudhury 1998; Malone *et al.* 1987). Some researchers also advocate that electronic exchange may also reduce contracting and monitoring costs (Gurbaxani and Whang 1991), however, empirical evidence in this regard is limited. Procurement from Internet-based marketplaces can potentially provide cost savings to the buyers but they also pose an elevated risk. The Internet is impersonal

and may amplify sourcing risk when parties unknown to each other are involved in the exchange activity (Duh *et al.* 2001). Moreover, transacting over the Internet introduces security and privacy issues that may add to the overall sourcing risk (Han and Noh 2000). Further, laws related to Internet transaction are not well developed, which raises contract and liability issues. Due to these conditions, the potential cost savings may be nullified by the substantially higher risk of purchasing from an Internet-based electronic marketplace. For an in-depth analysis of this issue, it is important to assess what specific risks exist and how they are increased because the transaction will take place through an electronic marketplace. We address these questions next.

Transaction cost economics (TCE) posits that partners in an exchange relationship may act opportunistically if given a chance (Williamson 1979). This opportunism creates a transactional hazard, which adds to the total cost of using the market and may make it less desirable or even infeasible. Agency theorists recognize goal incongruence between the principal and the agent. They claim that adverse selection risk and moral hazard risk (which is similar to opportunism) may add to the agency costs. These risks may be significantly amplified, because the impersonal nature of purchasing through the Internet limits the buyer's ability to observe the seller's behaviour. This issue is further complicated because the legal framework that governs transactions through an electronic marketplace is still in its evolutionary stages.

Resource dependence theory points out that dependence on other organizations for resources introduces uncertainty in an organization's decision making; in particular its supply chain management. Following an effectiveness rationale, this theory proposes strategic inter-firm governance to manage uncertainty and dependence (Pfeffer and Salancik 1978). Based on interdependence typology (Thompson 1967), Kumar and van Dissel (1996) argue that electronic marketplaces depict pooled interdependence (pooled information resources). They propose that repudiation, authentication, security and integrity risks are salient in electronic marketplaces.

The organization's perception of the risk in using a particular channel plays an important role in channel selection (McCorkle 1990). The importance of security risk, privacy risk and legal risk has been emphasized for Internet purchasing (Han and Noh 2000; Jarvenpaa and Todd 1997; Schoder and Yin 2000). Thus, various types of sourcing risk have been proposed in the literature. Some are peculiar to purchasing from the Internet such as security, privacy, repudiation, and authentication risk. Other risks such as moral hazard, adverse selection, legal, and performance risk are present in offline marketplaces but are elevated due to the use of the electronic medium for mediating transactions.

These research perspectives also provide insights into the control systems that can be employed to manage

sourcing risk. TCE and agency theory advocates contract design and monitoring as control systems, wherein the control choice is based on efficiency considerations (Gurbaxani and Whang 1991). Trust is another control option that has been proposed. It has been suggested that building trust is critical in transactions involving uncertainty, complexity or risk (Shapiro 1987). Trust may be viewed as a risk reduction mechanism that reduces transaction and agency costs. Some researchers argue that accreditation, feedback, monitoring and legal bonds may engender impersonal trust (based on institutional and structural arrangements) that may facilitate exchange activity through electronic marketplaces by reducing sourcing risk (Pavlou 2002). Bons *et al.* (1994) propose a variety of technical encryption-based and organizational- (third party) based solutions to manage sourcing risk in electronic marketplaces. Thus, numerous control options exist that electronic marketplaces can use to make the trading environment conducive for conducting transactions.

Agency and sociology theorists suggest that sourcing risk may differ according to the stage of the exchange relationship. For example, at the supplier selection stage, risk of selecting a supplier that may act opportunistically or may not have the required capability to perform is prominent. But after the supplier has been selected and contract formulated, post-contract performance risk may become more salient. Thus, the control strategy of a firm may involve proactive controls, such as selection efforts and/or reactive systems, such as monitoring (Bergen *et al.* 1992; Coleman 1990). Access to information and access privileges to engage in various activities at different stages of the transaction process may act as effective controls to reduce sourcing risk. This points toward the importance of the transaction process as an important dimension in understanding the various types of sourcing risk and control systems (Lee and Clark 1997; Rohem and Pernul 2000). Research also posits that controls invoked at various stages of the transaction process may act as substitute for each other. To the extent that such substitution effects exist, this could aid companies in developing efficient and effective control strategies (Picot *et al.* 1995).

Sourcing risk may also differ based on the type of electronic marketplace (Rohem and Pernul 2000). Seller-side or buyer-side marketplaces are relatively closed systems that allow contracting among known parties. Such electronic marketplaces by design control some sources of risk. On the other hand, public electronic exchanges (neutral hubs) are open systems that exert less control over participation. We explicitly focus on electronic marketplaces that serve as 'neutral hubs' and provide support for buyers and sellers equally (Archer and Gebauer 2002). Such an approach allows us to capture sourcing risk and control systems in a comprehensive fashion. Consequently, within the context of the proposed framework the type of electronic marketplace

may amplify or reduce the importance of certain sourcing risk and control systems.

The review of the literature raises some interesting issues:

- A buyer may face different types of source risk while purchasing from an Internet-based electronic marketplace. Current literature does not offer an approach for parsimoniously capturing the various facets of sourcing risk.
- Sourcing risk may differ based on the transaction process, so exploring which risk is salient in what stage of the transaction process can provide interesting insights.
- Various control systems have been presented for mitigating sourcing risk. But, limited attention has been directed towards investigating the relationship between sourcing risk and control systems in the context of Internet-based electronic marketplaces.
- Do control systems invoked at early stages of the transaction process act as substitutes for controls at the later stages and vice versa?

RESEARCH FRAMEWORK

The first issue is to develop a simple approach to capture various sources of risks. It can be argued that sourcing risk may relate to the supplier and/or the use of the electronic channel. We categorize sources of risk highlighted by previous research as specific to transacting with a supplier into transaction risk. Transaction risk is defined as the buyer's perception of risk that a supplier may not meet his/her commitments and promises. Based on this definition moral hazard risk, adverse selection risk, legal risk, repudiation risk, post-contractual performance risk, and post-contractual conflict risk that are all associated with the supplier can be grouped into transaction risk.

We categorize the risks peculiar to the electronic channels into security and privacy risks. Security risk is defined as the buyer's perception of risk regarding unauthorized access to the trading platform and the data residing in the system. So, authentication risk and data security risk can be categorized into security risk. Privacy risk is defined as the buyer's perception of risk towards exposure of sensitive information and misuse of sensitive information on their trading activities. Privacy risk constitutes the risk of information visibility and misuse of information collected by the Internet-based electronic marketplace.

It was suggested earlier that sourcing risk might differ based on the transaction process. This insight enables us to relate the various types of sourcing risk to the different stages of the transaction process. So, sourcing risk and transaction process constitute the two dimensions of the framework. Sourcing risk consists of transaction

risk, security risk and privacy risk (Figure 1). The transaction process comprises identification stage, negotiation and contracting stage, and settlement stage (Choudhury *et al.* 1998; Heide 1994; Lee and Clark 1997; Schubert and Selz 1997). Transaction risks may differ based on the stage of the transaction process, but security and privacy risks transcend the entire process. Thus, we only discuss transaction risk and controls within the context of the transaction process (Table 2 and Table 3). Next, we provide an in-depth review on the linkage between types of sourcing risk and control systems that may be used to mitigate them.

Identification Stage and Transaction Risk

The identification stage involves supplier search and supplier selection (Choudhury *et al.* 1998; Schubert and Selz 1997). Electronic marketplaces include

capabilities for helping firms in identifying potential trading partners (Choudhury *et al.* 1998). At this stage market participants can use the electronic marketplace to obtain information on potential trading partners that best fit their preferences (Lee and Clark 1997).

Electronic marketplaces open buyers to a host of suppliers with whom they previously may not have transacted. This along with minimal social context increases transaction risk at the identification stage. Transaction cost economics and agency theory suggests that adverse selection and moral hazard risks are salient at this stage (Stump and Heide 1996). Adverse selection risks arise from trading with a supplier who lacks the ability to perform. For instance, buyers procuring through electronic marketplaces may make purchasing decisions based on incomplete and possibly distorted information, without physically inspecting products. Such risks can be mitigated through effective qualification programs that assess a supplier's ability to perform.

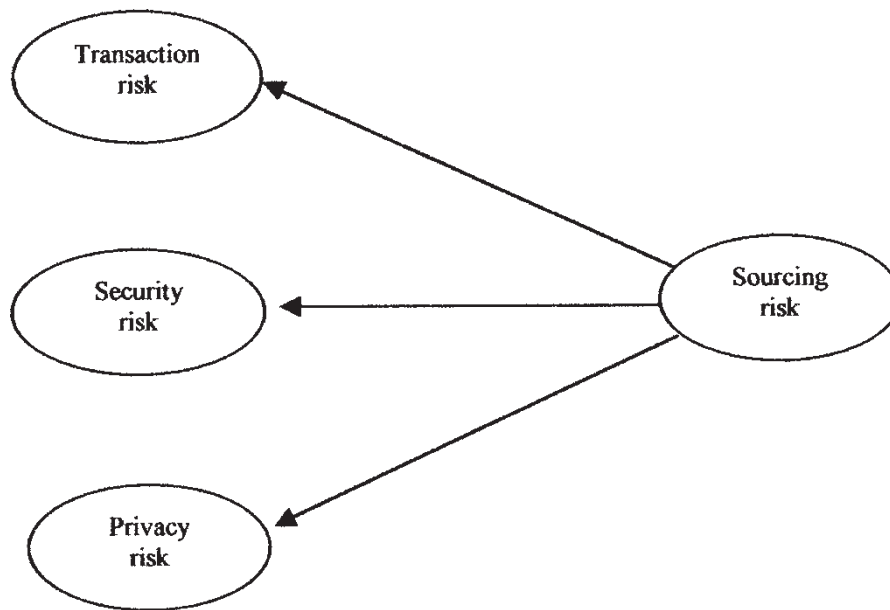


Figure 1. Dimensions of sourcing risk

Table 2. Sourcing risk

| Transaction process/risks | Sourcing risk | | |
|---------------------------|---|---------------------------------|--|
| | Transaction risk | Security risk | Privacy risk |
| Identification | Adverse Selection Moral Hazard | Authentication Data security | Information visibility Information collection |
| Negotiation & Contracting | Contract-legal Repudiation | Authentication Data security | Information visibility Information collection |
| Settlement | Post-contractual performance Post-contractual conflict | Authentication Data security | Information visibility Information collection |

Table 3. Sourcing risk

| <i>Control systems</i> | | | |
|-------------------------------------|--|--|--|
| <i>Transaction process/controls</i> | <i>Transaction controls</i> | <i>Security controls</i> | <i>Privacy controls</i> |
| Identification | <ul style="list-style-type: none"> • Qualification system • Inspection and product rating system • Reputation system | <ul style="list-style-type: none"> • Authentication systems (passwords and digital certificates) • Data security systems (encryption, digital signature, firewalls) • Backup strategy • Recovery systems (Recovery and restart procedures) | <ul style="list-style-type: none"> • Privacy policy (disclosure of information collected and its probable uses) |
| Negotiation and contracting | <ul style="list-style-type: none"> • Structured policy for roles, responsibilities and obligations • Insurance program • Date and time stamped documents with digital signature • Non-repudiation system | <ul style="list-style-type: none"> • Authentication systems (passwords and digital certificates) • Data security systems (encryption, digital signature, firewalls) • Backup strategy • Recovery systems (recovery and restart procedures) | <ul style="list-style-type: none"> • Privacy policy (disclosure of information collected and its probable uses) |
| Settlement | <ul style="list-style-type: none"> • Status monitoring system • Structure policy for dispute resolution | <ul style="list-style-type: none"> • Authentication systems (passwords and digital certificates) • Data security systems (encryption, digital signature, firewalls) • Backup strategy • Recovery systems (recovery and restart procedures) | <ul style="list-style-type: none"> • Privacy Policy (disclosure of information collected and its probable uses) |

Qualification programs can be similar to supplier selection procedures currently used by companies to screen suppliers. In addition, researchers have found inspection systems, standards and product rating systems to be effective controls (Watson and McKeown 1999).

Moral hazard risk captures the possibility that even capable suppliers may act opportunistically (Purdy *et al.* 1994). Research suggests that qualification programs that evaluate a supplier’s general customer practices and business philosophy may be effective (Ganesan 1994). Electronic marketplaces can provide the buyers access to information that they need for undertaking such qualifications (Duh *et al.* 2001). It can also offer buyers access to a reputation system based on customer feedback that rates the suppliers on previous customer dealings (Resnick *et al.* 2000). Such systems may parallel referencing and client list approaches typically employed by buyers in traditional markets.

For example, Converge.com, an electronic marketplace for electronic components, uses a qualification system that pre-qualifies sellers and their merchandize. Telcot, an electronic marketplace for cotton trading requires farmers (sellers) to send samples to the department of agriculture for determining grades based on a standardized system. A similar approach is being adopted

by American gem market systems. Since inspection systems may be costly, some electronic intermediaries have established franchise offices to overcome logistical issues.

Electronic marketplaces can team up with credit bureaus in offering real-time access to credit history information. They also have the option to use third party assurance services. For example, WebTrust service includes certification, which requires companies to disclose information about their business practices (Duh *et al.* 2001). The disclosure criteria include the time frame for order fulfilment, backorder notification, delivery methods, payment terms, complaint handling procedures and order cancellation procedures. Electronic marketplaces can also utilize the services of companies such as Harbinger Inc., a company that provides information to other organizations on the EDI capability of various firms (Khazanchi and Sutton 2001). Access to such services and systems can enable buyers to assess a supplier’s ability and intention to perform and thus reduce sourcing risk at this stage.

Negotiation and Contracting Stage and Transaction Risk

Once trading opportunities are discovered, the process 168

moves to negotiation and contracting. In this stage, buyers and sellers deliberate to reach an agreement on transaction price and terms of the contract (Lee and Clark 1997). In addition to verification of the information exchanged during the negotiation process, legal and contractual provisions are also important.

Researchers have pointed out that legal risk is a major impediment to online purchasing (Schoder and Yin 2000). This risk pertains to the online designation of responsibility and settlement of contracts and their enforcement. Inadequate means of tracing responsibility and verifying online transactions often result in a lack of legal liability. Contract signing procedures and their subsequent use as evidence must be considered. Such risks arise due to ambiguity about legal positions and options available to contracting parties. A well-articulated framework for assigning roles, responsibilities and obligations with clear legal position and options can be instrumental in controlling legal risk (Bakos 1998). In addition, insurance programs may also provide protection against such risk. Chemconnect.com has established exchange specific terms and conditions for contracts. These terms and conditions provide the legal framework for transactions conducted through their systems. Converge.com not only has its own terms and conditions for the contract but also allows participants the option of using Escrow Services (a company that provides contract formulation and settlement services).

Kumar and van Dissel (1996) note that market transactions carry contractual, performative and negotiative information. Within the context of electronic marketplaces this information may be subject to repudiation by either party. Thus, they emphasize the need to document all aspects of electronic market transactions. Procedures for storage of and access to documentation and messaging related to contracts and negotiations with date and time stamping may help alleviate the risk of repudiation. Transaction processing integrity procedures, document certification procedures, proof of delivery, and use of a digital signature may be part of these non-repudiation procedures (Rohem and Pernul 2000). Coverge.com has a system in place that ensures accuracy and inclusion of information and its associated processing methods. This requires the processor of electronic information to be able to prove his or her ownership or right to process and validates origination and receipt of information so that completed transactions cannot be repudiated. Third party services can also be used. For example, transaction integrity is one of the components, WebTrust uses to require certified companies to disclose information about controls that are in place to ensure transaction integrity. Verisign's digital trust services framework includes a digital signature as a mechanism for secure messaging. Digital signature indicates the identity of the person signing the document, message or record, and by attaching it assures that data has not been changed, destroyed, or lost.

Settlement Stage and Transaction Risk

The settlement stage involves the necessary exchange of information that clears the transaction through exchange of goods and payment (Lee and Clark 1997). In other words, the transaction participants finally clear their obligations as described in the contract.

Information asymmetry between contracting parties may expose buyers to shirking behaviour after order placement (Lal 1990). This leads to post-contractual performance risks that emerge from lack of information that determines whether a supplier's order fulfilment process is in line with their contractual obligations. In controlling this risk, buyers frequently monitor supplier's compliance to established standards of quality, delivery and other aspects of performance (Leenders and Fearon 1993). In the electronic marketplace context, the availability of a system that allows monitoring of order status may be an effective control mechanism for mitigating this risk. Converge.com provides buyers with delivery tracking services by partnering with shipping companies. Other types of tracking options also exist. For example, Savi Technologies by using RFID technologies (Radio Frequency Identification) tracks individual products, containers and transportation vehicles. The information is put on a common Internet platform for access. In addition to tracking delivery, post-purchase inspection services are also being offered. Many online marketplaces provide such services on their own or in collaboration with an escrow system. Escrow, as an independent third party, withholds the payment to the supplier in 'escrow', until the buyer upon receipt of the order has inspected the goods, and confirms that the goods are acceptable.

Another risk to buyers is post-contractual conflict. This risk often arises as a result of disagreement regarding expected and actual performance. Post-contractual conflict risk may be mitigated through effective arbitration and dispute settlement procedures (Bakos 1998). Recently, the American Arbitration Association has developed a dispute management protocol that can help online marketplaces resolve conflicts that may arise between buyers and sellers.

Transaction Process and Security Risk

Security risks transcend the entire transaction process. Kumar and van Dissel (1996) argue that in conducting transactions through electronic marketplaces, parties are exposed to authentication risk. Firms conducting electronic transactions may not always know the identity of the other party with certainty. As a result, authentication risk is an important component of the security risk. In addition, electronic transmission and storage of transaction related information exposes both parties to data security risk. Most of the transactions take place

over public electronic channels where the possibility of another party tapping the data transmission is real. In addition, the electronic marketplace as a third party mediator of the transactions may store transaction-related data, which may be subject to hacker attacks and system failure (Han and Noh 2000).

Systematic security risk management processes tailored to an Internet environment are effective control systems in mitigating security risk (Rohem and Pernul 2000). Electronic marketplaces can employ authentication systems for assuring the identity of the parties and use encryption methods (i.e. DES, AES and RSA) for security of data transmission. Secure Socket Layer (SSL) standard and Secure Electronic Transaction (SET) standard are comprehensive systems that address security issues. SSL protocol adequately prevents eavesdropping and manipulation of online messages and transactions, but does not address the authentication issue effectively. SET protocol is more comprehensive because it also incorporates authentication features.

In addition to authentication, security and integrity of stored data also needs to be considered. Firewalls, effective backup and recovery systems are some options that can ensure data security and integrity (Oppliger 1997). Firewalls can be used to enforce access control policies between networks and allow real time monitoring and intrusion detection systems for data security. Backup strategies can be developed depending on the demands being placed on the system and recovery and restart procedures can assure data integrity.

Converge.com has adopted a comprehensive set of security policies and controls to manage security risk. These controls and policies are aimed at proper identification and authentication of users and providing adequate protection for confidential or sensitive transaction-related data. These controls also cater towards protecting and securing against damage to, or loss of, information and unauthorized access.

Transaction Process and Privacy Risk

Organizations using electronic marketplaces may be concerned about the type of information collected by the market operator and how this information may be used. Market operators can potentially record navigational information, which, when combined with actual transactional data, may provide insights into buying patterns (Friedman *et al.* 2000). Increasing use of electronic marketplaces may also increase the visibility of an organization's buying behaviour. Such conditions lead to information collection and information visibility risks (Weiler 1995).

A well-structured privacy policy that elaborates on the information collected by the market operators, its permissible uses, control over data accessibility, and recourse in case of privacy breach could act as an

effective control mechanism (Cranor 1999). Electronic marketplaces can provide a self-developed privacy policy or adopt a third party solution. Companies such as eTRUST and BBB allow firms to display a privacy seal which provides assurance to buyers that electronic marketplace policies reflect their practices and options to recourse in case of a breach of policy. Electronic marketplaces can also enforce self-developed privacy policies that explain the type of information being collected and its allowable uses. For example, Converge.com's privacy policy explicitly identifies the type of information collected and elaborates that only aggregate level data may be disclosed to certain parties with the approval of the market participant.

Interdependencies among Control Systems

Previous research indicates that control systems are functionally dependent (Coleman 1990; Ouchi 1979). For example, if intensive efforts are made in carrying out supplier selection procedures, it may reduce the need for supplier monitoring during order execution (Casson 1991). Under such circumstances, monitoring may be redundant and add to the overall cost of contracting (Stump and Heide 1996). This typology of proactive and reactive controls is supported by studies within the context of sociology, agency theory and intra-organizational control (Bergen *et al.* 1992; Coleman 1990; Jaworski 1988). It is often denoted in accounting literature as prevention, detection and correction controls. Substitution effects among control systems may also be prevalent within the exchange activity in the electronic marketplace context. This can be extremely helpful in developing an efficient and effective control strategy. An important point to note here is that trade offs may only exist within the context of transaction risk because such risks vary by transaction stage. Security risk and privacy risk transcend the transaction process so these trade offs may not exist.

Effective controls, which enable rigorous screening of a supplier's ability and motivation to deliver on their promise, may, if provided to buyers at the identification stage, reduce the need for subsequent contract negotiation and post-contractual settlement controls. In addition, effective controls at the contracting and negotiation phase may reduce the control needs at the settlement stage. For example, it is common practice to engage in prearranged settlement activities such as 'evaluative receipt settlement'.

CONCLUSION

Sluggish adoption of Internet-based electronic marketplaces has raised questions about their viability as successful business models. Peculiar characteristics of

the Internet purchasing process can elevate sourcing risk. Identification of sourcing risk and the institution of control systems to alleviate such risk can be instrumental in increasing adoption and use of electronic marketplaces.

By integrating risk and control literature, this paper proposes a risk-control framework that links sourcing risk and corresponding control systems in the procurement context of the Internet-based electronic marketplaces. The framework segments sourcing risk into three categories: (i) transaction risk; (ii) security risk; and (iii) privacy risk. This framework further proposes that transaction risks differ based on the stage of the transaction process.

Effective control systems such as qualification system, product rating system, and reputation system may help in mitigating transaction risk at the identification stage of the transaction process. Transaction risk at the negotiation and contracting stage can be alleviated through non-repudiation systems, digital signature, institution of a legal framework, and insurance programs. Monitoring systems and dispute resolution protocols can be used as effective controls for managing post-contractual performance and conflict risks. A comprehensive security system that includes encryption techniques, digital certificates, firewalls, backup strategies, and recovery and restart procedures can be used to manage security risk. Complete disclosure of the type of information collected and its probable uses can mitigate privacy-related risk. We also point out that electronic markets have the option of using third party services in instituting control systems. WebTrust, Credit Bureaus, BBB, eTrust, Escrow Services, and Verisign are some of the options available and may provide unique services that bolster various control systems. The model also proposes that effective control at the identification stage of the transaction process may reduce the need for controls in the later stages. This assertion corroborates earlier research that proposes that extensive pre-selection efforts may reduce the need for subsequent monitoring.

The success of Internet-based electronic marketplaces hinges on the efficient and effective performance of the market functions. This paper proposes a framework that can help electronic market operators recognize sourcing risk and deploy control systems for facilitating procurement activities. By doing so, electronic market operators can facilitate the execution of market functions and entice buyers to participate. Although the framework builds on previous research findings, it needs empirical validation. Each link between sourcing risk and corresponding control system is a testable hypothesis. So, future research can focus on empirically testing the proposed framework. One option is to conduct an experiment, wherein buyers may be presented with vignettes that present situations with different levels of control systems in place. The buyers then may be asked to disclose their perception about various type of sourcing

risk and intention to purchase from an Internet-based electronic marketplace.

ACKNOWLEDGEMENT

The authors wish to acknowledge the helpful editorial comments of Jeff Milman on this paper.

References

- Anderson, E. and Weitz, B. A. (1992) 'The Use of Pledges to Build and Sustain Commitment in Distribution Channels', *Journal of Marketing Research* 29, 18–34.
- Archer, N. and Gebauer, J. (2002) 'B2B Applications to Support Business Transactions: Overview and Management Considerations', in Merrill Warkentin *Business to Business Electronic Commerce: Challenges and Opportunities*, Idea Group Publishing, 22–50.
- Bakos, J. Y. (1991) 'A Strategic Analysis of Electronic Marketplaces', *MIS Quarterly* September, 295–310.
- Bakos, J. Y. (1998) 'The Emerging Role of Electronic Marketplaces on the Internet', *Communications of the ACM* 41(8), 35–42.
- Bergen, M., Dutta, S. and Walker, O. C. (1992) 'Agency Relationships in Marketing: A Review of the Implications and Applications of Agency and Related Theories', *Journal of Marketing* 56, 1–24.
- Bons, R. W. H., Lee, R. M. and Wagenaar, R. W. (1994) 'Implementing International Trade Using Open-EDI', EURIDIS Working Paper.
- Casson, M. (1991). *The Economics of Business Culture: Game Theory, Transaction Costs, and Economic Performance*, New York: Oxford University Press.
- Choudhury, V., Hartzel, K. and Konsynski, B. (1998) 'Uses and Consequences of Electronic Markets, An Empirical Investigation in the Aircraft Parts Industry', *MIS Quarterly* 22(4), 471–507.
- Clemons, E. K., Reddi, S. P. and Row, M. C. (1993) 'The Impact of Information Technology on the Organization Activity: The Move to the Middle Hypothesis', *Journal of Management Information Systems* 10(2), 9–35.
- Coleman, J. S. (1990) *Foundation of Social Theory*, Cambridge, MA: Harvard University Press.
- Cranor, L. F. (1999) 'Internet Privacy', *Communication of the ACM* 42(2), 28–31.
- Dowing, G. R. and Staelin, R. (1994) 'A Model of Perceived Risk and Intended Risk-handling Activity', *Journal of Consumer Research*, 21, June, 119–34.
- Duh, R. R., Jamal, K. and Sunder, S. (2001) 'Control and Assurance in E-commerce: Privacy, Integrity and Security at eBay', American Accounting Association.
- Friedman, B., Kahn, P. H. and Howe, D. C. (2000) 'Trust Online', *Communications of the ACM* 43(12), 34–40.
- Ganesan, S. (1994) 'Determinants of Long-Term Orientation in Buyer-Supplier Relationships', *Journal of Marketing* 58, 1–19.
- Grazioli, S. and Jarvenpaa, S. (2000) 'Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with

- Experienced Internet Consumers', *IEEE* 30(4), 395–410.
- Gurbaxani, V. and Whang, S. (1991) 'The Impact of Information Systems on Organizations and Markets', *Communications of the ACM* 34(1), 59–73.
- Han, K. and Noh, M. (2000) 'Critical Failure Factors that Discourage the Growth of Electronic Commerce', *International Journal of Electronic Commerce* 4(2), 25–43.
- Heide, J. B. (1994) 'Inter-organizational Governance in Marketing Channels', *Journal of Marketing* 58, 71–85.
- Heide, J. B. and John, G. (1990) 'Alliances in Industrial Purchasing, The Determinants of Joint Action in Buyer–Supplier Relationships', *Journal of Marketing Research* 27, 27–36.
- Jarvenpaa, S. and Todd, P. (1997) 'Consumer Reactions to Electronic Shopping on the World Wide Web', *International Journal of Electronic Commerce* 1(2), 59–88.
- Jaworski, B. J. (1988) 'Toward a Theory of Marketing Control: Environmental Context, Control Types and Consequences', *Journal of Marketing* 52(3), 23–39.
- Khazanchi, D. and Sutton, S. G. (2001) 'Assurance Services for Business-to-Business Commerce: A Framework and Implications', *Journal of the Association of Information Systems* 1, 11.
- Kumar, K. and van Dissel, H. G. (1996) 'Sustainable Collaboration: Managing Conflict and Cooperation in Inter-organizational Systems', *MIS Quarterly*, September, 279–300.
- Lal, R. (1990) 'Improving Channel Coordination through Franchising', *Marketing Science* 9(4), 299–318.
- Lee, H. G. and Clark, T. H. (1997) 'Marketing Process Reengineering Through Electronic Market Systems: Opportunities and Challenges', *Journal of Management Information Systems* 13(3), 113–36.
- Leenders, M. R. and Fearon, H. E. (1993) *Purchasing and Materials Management*, 10 edn, Homewood, IL: Richard D. Irwin.
- Malone, T. W., Yates, J. and Benjamin, R. I. (1987) 'Electronic Markets and Electronic Hierarchies', *Communications of the ACM* 30(6), 484–497.
- McCorkle, D. E. (1990) 'The Role of Perceived Risk in Mail Order Catalog Shopping', *Journal of Direct Marketing* 4, 26–35.
- Oppliger, R. (1997) 'Internet Security: Firewalls and Beyond', *Communications of the ACM* 40(5), 92–102.
- Ouchi, W. A. (1979) 'Conceptual Framework for the Design of Organizational Control Mechanisms', *Management Science* 25(9), 833–48.
- Pavlou, P. (2002) 'Impersonal Trust in B2B Electronic Commerce: A Process View', in Merrill Warkentin *Business to Business Electronic Commerce: Challenges and Opportunities*, Idea Group Publishing, 71–90.
- Pfeffer, J. and Salancik, R. (1978) *The External Control of Organizations: A Resource Dependence Perspective*, New York: Harper & Row.
- Picot, A., Bortenlaenger, C., Roehrl, H. (1995) 'The automation of capital markets', *Journal of Computer Mediated Communication* 1(3), online at: <http://www.ascusc.org/jcmc/vol1/issue3/picot.html>
- Purdy, L., Astad, U. and Safayeni, F. (1994) 'Perceived Effectiveness of the Automotive Supplier Evaluation Process', *International Journal of Operations and Production Management* 14(6), 91–103.
- Resnick, P., Zeckhauser, R., Friedman, E. and Kuwabara, K. (2000) 'Reputation Systems', *Communications of the ACM* 43(12), 45–8.
- Rindfleisch, A. and Heide, J. (1997) 'Transaction Cost Analysis: Past, Present and Future Applications', *Journal of Marketing* 61, October, 30–54.
- Rohem, A. W. and Pernul, G. (2000) 'COPS: A Model and Infrastructure for Secure and Fair Electronic Markets', *Decision Support Systems* 29, 243–355.
- Sarkar, M. B. Bulter, B. and Steinfield, C. (1996) 'Intermediaries and Cybermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace', *Journal of Computer Mediated Communication* 1(3), online at: <http://www.ascusc.org/jcmc/vol1/issue3/sarkar.html>
- Schoder, D. and Yin, P. L. (2000) 'Building Firm Trust Online', *Communications of the ACM* 43(12), 73–9.
- Schubert, P. and Selz, D. (1997) 'Web Assessment – Measuring the Effectiveness of Electronic Commerce Sites Going Beyond Traditional Marketing Paradigms', *Electronic Markets* 7(3), 46–8.
- Shapiro, S. P. (1987) 'The Social Control of Impersonal Trust', *American Journal of Sociology* 93, 623–58.
- Sklar, D. (2001) 'Building Trust in an Internet Economy', *Strategic Finance* April, 22–5.
- Stump, R. L. and Heide, J. B. (1996) 'Controlling Supplier Opportunism in Industrial Relationships', *Journal of Marketing Research* XXXIII, 431–41.
- Thompson, J. (1967) *Organizations in Action*, New York, NY: McGraw Hill.
- Watson, R. T. and McKeown, P. G. (1999) 'Manhiem Auctions: Transforming Inter-organizational Relationships with an Extranet', *International Journal of Electronic Commerce* 3(4), 29–46.
- Weiler, R. M. (1995) 'Money, Transactions and Trade on the Internet', *Imperial College*, London, online at: www.graph.ms.ac.uk./results
- Williamson, O. (1979) 'Transaction Cost Economics: The Governance of Contractual Relations', *Journal of Law and Economics* 22(2), 233–261.