ISeB (2004) 2:31–55
DOI 10.1007/s10257-003-0026-y

Information
Systems
and
e-Business
Management

Measuring dimensions of perceived e-business risks

Judy E. Scott

The Business School, University of Colorado at Denver, Campus Box 165,
P.O. Box 173364, Denver, CO 80217-3364, USA (e-mail: judy.scott@cudenver.edu)

Abstract. The risks to e-business from breaches of security and privacy are well known. However, research has given very little attention to other important e-business risks. Using a socio-technical approach, in this study we survey a diverse sample of almost 200 participants to rate their perception of 16 e-business risks, compiled from the research and practitioner literature. Strategic risks, organizational risks and e-business policy risks emerged as the three underlying dimensions of e-business risk. In terms of the socio-technical model, strategic risks focus on the actor-structure component, and policy risks focus on the task-structure component. Organizational risks cover a wide spectrum of socio-technical components such as technology, actor-technology, technology structure and task-actor. The main contribution of this study is a multi dimensional scale of e-business risk perception. Practitioners can benefit by focusing their risk management efforts on the three dimensions of e-business risk, which are easier to manage than a long checklist of unrelated risks. Researchers benefit from a raised awareness on the importance of strategic and organizational risk factors in addition to policy risk factors for e-business risk management. A model that incorporates the three dimensions of e-business risks and shows theoretically based relationships with control mechanisms, trust, perceived uncertainty and profitability is proposed for testing in future research.

Key words: e-business, risk, control, trust, uncertainty

1 Introduction

Failed dot-coms underestimated the risks of doing e-business. When Webvan went out of business in July 2001, investors lost $1.2 billion and 2000 employees lost their jobs. Several questions are left unanswered. What are perceived risks of conducting e-business? Are the risks specific to e-business or applicable to business in general? The risks of participating in e-business are diverse, yet research has not yet established a ranking of perceived e-business risks, nor a multi dimensional scale of these risks.

Financial losses from security violations, such as denial-of-service attacks and credit card postings by hackers (Duffy 2000), as well as privacy violations (Van Mien 2000) are well known. These e-business risks damage an organization's reputation and result in the loss of thousands of potential customers (Iwata 2000). In December 1999, hackers posted thousands of credit card numbers, with expiration dates, names and addresses. They had stolen 300,000 credit-card numbers from online music retailer CD Universe (Dekleva 2000, Sager 2000), who refused to pay the $100,000 ransom. Yahoo!, Amazon.com, eBay, CNN.com and eTrade lost an estimated $1.2 billion from denial-of-service attacks in February 2000 (Beard and Ehrenreich 2000). In March 2000, calling card numbers were stolen from several large phone companies at an estimated $2 million loss (Sager 2000).

Organizations reported 43,136 security incidents to the Computer Emergency Response Team during the first and second quarters of 2002 (CERT 2002). That compares with 52,658 for all of 2001, 21,756 in 2000 and 9,859 in 1999. In a recent study, 90% of the 503 respondents from large corporations and government agencies said they had suffered some sort of security breach in the past 12 months. The average financial toll has risen to $2 million per instance from $500,000 in 1997 (Salkever 2002). The total annual cost of online security breaches to corporations in the U.S. is estimated at $15 billion (Computerworld 2001). Estimates suggest that viruses alone have caused worldwide damage reaching $11 billion due to lost employee productivity, downtime and data loss (Dean and Carey 2000). In March 2000, the Melissa virus caused an estimated $80 million in damage when it swept around the world, paralyzing e-mail systems (Sager 2000). The Nimda or Code Red worms that emerged in the summer and fall of 2001 caused more than $2 billion in clean-up expense and lost productivity (Lemke 2002).

Internet fraud is increasing. According to the National Consumers League, one-fourth of all its consumer complaints are now about the Internet, up from just three percent in 1997. Individuals and businesses lost $3.2 billion in 2000. Card-not-present fraud - committed over the Internet, telephone, or fax grew by 117% (M2 Presswire 2000). Expedia set aside $6 million for credit card fraud in 1999 (Patient 2000). In mid-2001, Visa had a 12 times higher incidence of Internet transaction fraud than in-store fraud (Pescatore 2002). The Federal Trade Commission identified 18,660 instances of potential Internet fraud in 2000. At the Securities and Exchange Commission, officials receive about 2,000 e-mails a day identifying potential Internet fraud (Lord et al. 2001).

Privacy violations include use of cookies and web bugs by Doubleclick, Matchlogic and Avenue A to collect information on consumers without their consent. RealNetworks surreptitiously collected information about its users, embedding the global unique identifier in RealJukebox, making it possible to track users on the Web (Dekleva 1999).

Threats to e-business come from security violations, privacy violations, ruined reputation, identity theft, loss of intellectual property, and difficulty identifying people on the Internet. In addition to risks that are specific to e-business, conducting e-business on a global scale introduces issues associated with diverse cultures, legislation and currency. Similar to traditional business, there are risks from elusive profitability, poor strategy, inadequate leadership and cutthroat competition. Too much dependency on vendors or

other third parties, lack of reliability of technology and unavailability of expertise are other risks.

Prior research has addressed many aspects of e-business risks associated with strategy, leadership, reputation, culture, security, privacy and technology. Nevertheless, there is a gap in an overall theory and empirical research is needed to categorize the risks so that research can move towards frameworks and models. This study's objective is to rank perceived e-business risks, develop a multi dimensional scale of perceived e-business risks, investigate the impact of demographic variables on perception of e-business risks and propose a model for the control of e-business risks.

Sixteen e-business risks were identified from the research and practitioner literature. Respondents to an online survey were asked to rate their perception of each of these risks. Profitability, privacy and security received the highest ranking. Analysis of demographic data showed that, with a few exceptions, overall the risks were perceived similarly regardless of differences in functional area, job responsibilities, job role, age or gender. A factor analysis revealed three dimensions of e-business risk associated with strategic, organizational and e-business policy risks. The findings raise awareness of the importance to e-business of strategic and organizational issues, such as leadership and reputation, which have been overshadowed by security and privacy issues. Building on these three dimensions, we propose a model for control of e-business risks.

In the following section of this paper, we discuss a theoretical background on e-business risks, focusing on strategy, culture, technology, leadership, reputation, privacy, identity, intellectual property and security. Based on the literature review, we propose a list of e-business risks in terms of socio-technical components. The third section has the methodology used to collect and analyze data on perceptions of e-business risks. The fourth section contains the results of the demographic and factor analysis. The fifth section is the discussion and in the final section we conclude the paper with implications for management and research.

2 Theoretical background

Uncertainty, trust and control are recurring themes in risk research (Barki et al. 1993, Nidumolu 1996, Hine and Eve 1998, Milberg et al. 2000, Palmer, Bailey and Faraj 2000, Smith et al. 2001). The higher the perceived uncertainty, the greater the perceived risk. Trust and control mechanisms lower the perceived uncertainty and consequently the perceived risk.

There are multiple dimensions of trust, control mechanisms, perceived uncertainty and e-business risks. Trust has dimensions such as cognitive, which is objective, and affective, which is based more on feelings (McAllister 1995). Since affective trust is usually facilitated face-to-face, cognitive trust is more applicable to e-business. Cognitive trust in e-business would be generated by control mechanisms that increase reliability measures, such as monitoring compliance to privacy legislation. Establishing trust would overcome consumers' fear in transacting over the Web, a major obstacle for e-business (Rose et al. 1999). The marketing literature on perceived risks suggests that consumers are concerned about the performance of the product,

as well as financial, time, psychological and social risks (Cunningham 1967). The inability to observe and hear the merchant and to touch the merchandise exacerbates uncertainty for the potential e-business customer. It is difficult to assess the trustworthiness of a trading partner due to limited sensory inputs and limitations of the medium. The information asymmetry may give rise to opportunistic behavior (Tan and Thoen 2000). For example, consumers might not receive the product or might be disappointed with the received goods. From the perspective of the e-business, control mechanisms, such as policies, technology tools, and regulation, reduce uncertainty and risk (Alavi and Weiss 1985, Barki et al. 2001).

System development risks have been categorized using Levitt's socio-technical model (Lyytinen et al. 1998). Similarly, in this study we use a socio-technical approach. Task, technology, structure and actor components of the model and their interactions characterize risks. See Fig. 1. In the following section, we discuss the literature relevant to multiple dimensions of e-business risks and summarize the risks in terms of Levitt's socio-technical model.

2.1 Reliability of technology risk to e-business

In e-business, uncertainty arises from reliance on new technology and vulnerability to rapid changes in technology (Gefen 2002, Moscove 2001). New, immature and constantly changing technology is often unreliable (Barki et al. 1993, Lyytinen et al. 1998, Willcocks et al. 1999, Schmidt et al. 2001, Scott and Vessey 2002). E-business is especially vulnerable to an inadequate infrastructure because of its complete reliance on IT for commercial transactions (Ettredge and Richardson 2001). Moreover, technical security architectures (Schlarman 2002) need to be robust enough to prevent theft of electronic data (Moscove 2001) and costly denial-of-service attacks (Sabo 1998).

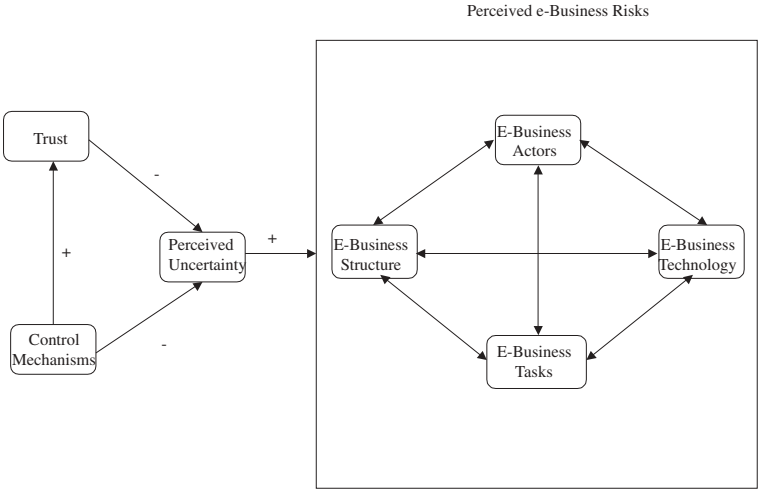

Fig. 1. Socio-technical model of perceived e-business risks

The importance of architecture (Weil et al. 2001) was highlighted during the 1999 Christmas season when e-tailers, including CDnow, KBkids.com, and Toysrus.com, failed to deliver toys and gifts in time, partly due to the lack of integration between their front-end and back-end systems. A study by PricewaterhouseCoopers in 1999 showed 93% of corporate Web sites were not linked to back-office operations (Saban 2001), so real time inventory was not available online. Similarly, a study by KPMG in 2000 showed lack of integration as the most formidable barrier to implementing an e-business strategically aligned with the traditional business.

2.2 Expertise risks to e-business

Uncertainty arises from a lack of experience in doing e-business (Rose et al. 1999, Kern et al. 2002). Belief in the competence of the e-business influences consumers' trust (Gefen 2002). In e-business, similar to traditional business, constant change leads to a shortage of expertise, which increases organizational risk (Barki et al. 1993, Lyytinen et al. 1998, Schmidt et al. 2001, Scott and Vessey 2002). Since skills become obsolete from a constant stream of new technologies, training and learning are critical.

2.3 Dependence risks to e-business

Entities outside the organization, such as customers, suppliers, software vendors, consultants, outsourcers and the government may provide needed expertise but put the organization at risk from over dependency (Willcocks et al. 1999). Management perceives uncertainty and a lack of control over external risks (Keil et al. 1998, Schmidt et al. 2001, Scott and Vessey 2002), such as government Internet intervention (Ettredge and Richardson 2001) and application service providers (Kern et al. 2002). Public acceptance of e-commerce, e-advertising and e-products is also uncertain. Nevertheless, trust and control mechanisms such as privacy policies, supplier monitoring and service level agreements with consultants and outsourcers, reduce uncertainty and risk.

2.4 Strategic risks to e-business

Although operating risks such as technology failures prevent business from being conducted, strategic risks are even more severe since they result in a loss of market share and render the company noncompetitive (Smith et al. 2001). An organization's inability to understand its strategic needs puts it at risk for internal conflict (Clemons et al. 1995). Several surveys reveal that strategic risks have been neglected in e-business (Saban 2001, Porter 2001). In 2001, a survey found 65% of respondents did not have an e-commerce strategy and yet were undertaking significant e-business activities (Ernst and Young 2001). Another survey found 24% of respondents did not have a written Internet business strategy, and 45% said such a plan was 'under development' (Potter 2000).

Both traditional businesses and dot-coms need an e-business strategy (Porter 2001). Traditional business needs to venture online and find synergies with its offline businesses. In the late 1990s, continuing to do business in the traditional way was perceived as high risk because of the threat that the Internet would transform industries, leaving incumbents worse off unless they adapted to the new paradigms (Saban 2001). IBM established a new division for its e-business strategy. J.C. Penney invested $200 million to build JCPenney.com in 1998 after its catalog division chief warned that doing nothing online might cost the firm $2 billion in sales by 2003 (Kaihla 2001).

2.5 Competitive risks to e-business

The pioneers in e-business expected a competitive advantage. Their highest priority was "getting big fast", based on the theory of network externalities, which explains the growth of networks as a "winner takes all" first mover advantage (Amit and Zott 2001). As a network grows and achieves a critical mass, it attracts more participants and becomes more valuable to the extent that other smaller networks cannot compete. This theory has held for auctions and is illustrated by the spectacular growth and dominance of eBay. On the other hand, low switching costs usually negate the advantage (Porter 2001) and many dot-coms erroneously grew too fast, when there was insufficient demand to justify their strategy. For example, Webvan had over-ambitious plans for national expansion that it scaled back too late to prevent its demise.

Organizations expected a competitive advantage from personalization that would lock-in their customers by raising switching costs (Amit and Zott 2001, Straub and Watson 2001). However, with a few exceptions such as Amazon, consumers usually switch quite readily to competitors' websites which are an easy click away. Furthermore the availability of software agents that compare products also discourages lock-in.

The gold rush mentality was also exemplified by the attitude of "build it and they will come." Market research was either disregarded or ineffective. Many dot-coms assumed that any type of product would sell on the Internet, and that consumers would instantly change their shopping habits for products such as groceries and furniture. They ignored the uncertainty that consumers would feel about not experiencing the "look and feel" of such products and the perceived risk of buying large ticket items with variable quality such as furniture (De Figueriedo 2000).

The survival rate of "brick-and-click" business models is higher than for pure dot-coms (Porter 2001). However, many start-ups did not see the need for an offline presence. They ignored the benefits of complementarities (Amit and Zott 2001), which explain the advantage for consumers of having a store where they can inspect goods and return products that are unsatisfactory.

2.6 Profitability risks to e-business

Profitability has been elusive for e-business, although eBay, priceline.com, Expedia and Travelocity.com are a few exceptions. The Internet alters industry structure often dampening overall profitability (Porter 2001).

During the boom the start-ups ignored traditional business principles related to strategy and profitability. Because venture capital was plentiful, profitability was sacrificed for gains in market share. Free or low prices subsidized with advertising were used to attract customers. Although a free pricing strategy is successful when it generates demand for another product (Kauffman and Walden 2001), early banner ads were generally ineffective. When economic problems reduced expenditures in 2001, business models that depended on online advertising, such as that used by buy.com (Porter 2001), became unviable.

2.7 Leadership risks to e-business

Leadership needs to set the vision, oversee the strategy and allocate resources (Saban 2001, Willcocks and Griffiths 1997). Research shows that top management guidance facilitates strategic use of IT (King and Teo 1996). Several surveys acknowledge the importance of leadership in e-business. Leadership needs to take an active role in managing e-business risks. They should not delegate all of the responsibility to the CIO, because changing employee behaviors and attitudes that affect corporate security, for example, needs buy-in and leadership from top management (Straub and Welke 1998, Duffy 2000).

Governance has always been important to business but was sometimes ignored by the start-ups (Weil et al. 2001). Controls tended to be lax and there are many examples of youthful dot-com ''executives'' who were technology savvy but lacked essential business experience and leadership skills. Although effective leadership is just as important for e-business as it is for traditional business, a survey in 2000 found that e-strategies were developed without strong leadership and decision-making at the executive levels. The survey concluded that the lack of leadership and vision was handicapping successful Internet business strategies (Potter 2000).

2.8 Reputation risks to e-business

The risk of ruining an organization's reputation can be severe. Customer service failures can soon become common knowledge, exacerbated in a ''24/7'' e-business environment. Online firms try to establish a good reputation to gain trust and reduce the quality risk associated with limitations of the electronic medium (Palmer et al. 2000). However, customers who perceive business practices as using their personal information unfairly may engage in bad word of mouth and may defect (Culnan and Armstrong 1999). Angry consumers may post negative comments to online discussion boards causing harm to the firm's reputation and hampering its ability to attract new customers. In 2000, consumer complaints prompted the Better Business Bureau to delist Priceline forcing it to improve its customer service to regain certification.

The failure to implement and monitor effective security procedures may threaten a Web site's information integrity (Camp 1999) and result in fraudulent use of information, adversely affecting corporate reputation. Reputation is also at risk because of loss of control when an organization is

dependent on a third party or outsourcing such as with an Application Service Provider (Porter 2001).

Reputation rating schemes such as third party certification and feedback mechanisms build trust (Kauffman and Walden 2001). User rankings on eBay prevent fraud in most cases, because negative ratings ruin a trader's reputation (Resnick et al. 2000, Zacharia et al. 2000). Similar to a Better Business Bureau, eBay posts buyers' ratings of their experience with a seller on its site. The system is not foolproof, however. Stewart Richardson had 6,170 positive ratings and only 43 negative ones when he conned $300,000 from eBay buyers (Freedman 2002).

2.9 Culture and currency risks to e-business

Organizations may have cultural problems in instituting e-business practices and ideas (Rose et al. 1999). Culture is particularly essential for global e-business. Organizations that go global must face issues such as cultural differences, currency conversion and the expertise needed for international transactions. Areas of diversity to contend with, include presentational issues, degrees of formality, payment methods, currency, regulation, governance, trading law, the meaning of contract, and semantics and lexicon language differences, both general and industry-sector-specific (Mitchener 2000).

Differences in consumer privacy concerns and use of legislation may be associated with cultural values, such as uncertainty avoidance (Milberg et al. 2000). In the EU, specific consumer opt-in is required for the reuse of personal information specifying, or from which can be deduced, medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or the sexual orientation of the individual (De Lotto 2001).

Although local currency is available in many global e-business Web sites, US dollars are sometimes used despite consumers' preference to know the price of goods in their local currency and the fact that currency conversion is relatively easy to automate.

2.10 Intellectual property risks to e-business

In 1998, the Department of Commerce reported that U.S. businesses incurred $12.5 billion in intellectual property losses (Dean and Carey 2000). Legal issues regarding patents, trademarks, trade secrets and copyrights, are collectively known as intellectual property issues (Deklava 2000). Patents such as Amazon's one-click and Priceline's "name your own price" are controversial. Because digital products can be reproduced for free and then distributed by anyone who has acquired an initial copy (Kauffman and Walden 2001), intellectual property is of particular concern to the music and entertainment industry, which perceives the Internet as a threat rather than an opportunity. Intellectual property concerns prompted legal action against popular online music site Napster resulting in its demise. The music industry is proposing technological methods of protecting copyright, such as the Secure Digital Music Initiative, which is described as an open set of

standards for the secure distribution of music in the Internet, and digital rights management such as digital watermarks and encryption technology (Anestopoulou 2001).

2.11 Identity risks to e-business

In e-business, uncertainty arises from an unverifiable location and anonymity (Gefen 2002, Moscove 2001). Transaction security needs guarantees of knowing to whom one is sending or from whom one is receiving data. Digital signatures, Secure Electronic Transaction (SET), and similar technologies can act as guarantors for the transaction, assuring interested parties that the signatories involved currently exist and are who they claim to be. Passport from Microsoft and the Liberty Alliance Project involving Sun and other companies protect against fraud by identifying customers.

From a consumers' perspective, identity theft threatens personal credit and may involve long-term expensive litigation (Berghel 2000). It is the fastest growing crime in the U.S. with over 500,000 cases reported each year. Identity theft enables financial fraud when enough personal information about an individual is amassed for a perpetrator to successfully masquerade as the victim and exploit his or her credit lines (De Lotto 2001). Control mechanisms, such as having identities hard coded onto a smart card and using biometrics such as retina scanners to confirm identities prior to authorization of use (Rose et al. 1999), make identity-theft extremely difficult. Since the September 11 terrorist attacks, the government has increasingly considered biometrics and identity cards to improve security. The Defense Department contracted with EDS for 360,000 smart cards to enable enlisted and civilian personnel physical access to secure bases and to log onto secure networks (Boyd 2001).

2.12 Security risks to e-business

Cybersecurity has become a national concern since the terrorist attacks. Security planning models help to cope with systems risk through deterrence, prevention, detection and remedies (Straub and Welke 1998). A framework can address the information cycle for the security process, by relying on information that is a combination of policies, controls for varying platforms, procedures, vulnerability alerts, regulatory standards, industry standards, information classifications, risk assessments, and technical security architectures (Schlarman 2002).

There are two types of protection – passive and active. Passive protection examples include virus scanning, encryption, and firewalls, while active protection examples include vulnerability analysis and intrusion detection (Smith et al. 2001). Access control services protect computing and networking resources from unauthorized use. Communication security services provide authentication, data confidentiality and integrity, as well as nonrepudiation services to communicating peers (Oppliger 1997).

Some security risks are unique to mobile devices, such as the risk of loss or theft (Ghosh and Swaminatha 2001). It is difficult to trace users of wireless devices, which roam in and out of wireless zones, have no fixed geographic point, and can go online and offline easily. Malicious downloads and

misinformation or simple denial of service can potentially compromise wireless devices.

Weaknesses in Internet security are often the failure to utilize existing security features of the Internet such as authentication and encryption (Radcliff 1997). Encryption is available through Secure Socket Layer (SSL) embedded in the browsers or through Secure Electronic Transmission (SET) being promoted by a consortium of credit card firms (Rose et al. 1999). Perfect security may have the tradeoff of severely limiting users in the accomplishment of their jobs (Huston 2001). High-profile interruptions of electronic securities trading at E*Trade and Charles Schwab and two subsequent class-action lawsuits against E*Trade have spiked interest in Internet-specific insurance policies, including denial of services coverage.

2.13 Privacy risks to e-business

Widespread use of data mining tools makes it relatively easy to compile a dossier about an individual from many different data sources, such as transaction records and records of an individual's click stream (Cranor 1999). Cell phones and other mobile devices can reveal an owner's location and enable marketers to send coupons for a participating merchant to the user while passing the merchant (Ghosh and Swaminatha 2001). Similarly, "OnStar" from GM will allow merchants to beam discounts offers when the driver is in the vicinity. Also invasive, is the collection of cell phone numbers for offline direct telemarketing. In March 2000, AT & T Wireless and Sprint PCS were sending users' cell phone numbers to the Web sites they had accessed (Ghosh and Swaminatha 2001).

As more personal information goes online, the risk of disclosure increases. Disclosure of electronic health records could affect employment decisions, and denial of insurance. Disclosure of electronic financial records could lead to financial fraud. Disclosure of social security numbers could lead to identity theft (Berghel 2000). Disclosure of contact information could result in spam and unwanted solicitations (Hinde 2002, Wang et al. 1998).

Technology-enabled personalization saves marketers time and money by targeting advertising and helps avoid annoying customers with irrelevant offers, easing information overload. However, a consumer needs to be motivated to disclose personal information actively by registering or filling out a form, and may resent the privacy intrusion and time and may falsify information (Hinde 2002). On the other hand, consumers may be passively unaware that their clickstream is being collected by the e-business (Hoffman et al. 1999).

Consumers resent losing control of personal information (Stewart and Segars 2002) and protest when their personal information is sold to third parties without their permission (Smith et al. 1996). This perception has not been helped by failed dot coms, such as Toysmart, attempting to sell their customer data to raise money to pay creditors. If organizations neglect to address customers' privacy concerns, then they risk losing demand for their products and services.

Organizations can address consumers' privacy concerns using procedural fairness, which builds trust (Culnan and Armstrong 1999). Announcing the site's privacy policy removes the uncertainty of what is done with consumers'

data, improves trust and allows consumers to make informed decisions about using the site and disclosing their personal information. However, a study on health websites found that, despite explicit privacy policies, instances of policy violation and deception occurred (Moscove 1991). Furthermore, an empirical study in 1999 showed that only 45 of the 102 firms investigated had privacy statements, only 17 firms used trusted third parties and only 3 of the 17 used both TRUSTe and BBB (Better Business Bureau) Online (Palmer et al. 2000).

2.14 Legal risks to e-business

Although the U.S. government's approach discourages e-business regulation (Dekleva 1999), there is concern about an ambiguous or hostile legal or regulatory environment (Rose et al. 1999), and perception that government Internet intervention is a risk largely out of firm's control (Ettredge and Richardson 2001). On the other hand, some individuals are more inclined to prefer government intervention (Milberg et al. 2000), expressing the opinion that self-regulation has failed (Hinde 2001) and that legislation and a publicly funded watchdog are essential (Clarke 1999).

Despite the moratorium on Internet tax extension until 2003 (Regan 2002), many consider taxation of Internet business is inevitable and want taxation mechanisms that encourage e-business growth without unfairly penalizing brick-and-mortar firms (Kauffman and Walden 2001). A country's regulatory approach to corporate management of information privacy is affected by cultural values and consumer concerns (Milberg, Smith, Burke 2000). Europe has stricter privacy laws than the U.S. The Safe Harbor agreement is an attempt to reach a compromise but according to some has had mixed results. As discussed earlier, the privacy of health records is critical. Mandatory compliance with the various components of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is currently scheduled for 2002 and 2003 although many health care organizations are pushing the U.S. Congress for a longer phase-in period (Huston 2001).

In summary, e-business risks are related to perceived uncertainty. Organizations can reduce perceived uncertainty by increasing trust and using control mechanisms. Using a socio-technical approach, we characterize the identified risks in terms of technology, actor, structure and task components and their interactions. See Table 1 for the rationale and characterizations. In the following section we describe the methodology for our empirical study.

3 Methodology

A first step in managing e-business risks is to gain a theoretical understanding of the construct. Measuring instruments for a construct identify the underlying dimensions for the construct. Factor analysis is the methodology typically used for exploring and verifying the dimensions and measures for a construct. In early stages of a line of research, exploratory factor analysis is more appropriate than confirmatory factor analysis because a model cannot yet be specified (Bagozzi 1981, Bollen 1989). During exploratory factor analysis, the factors are assigned meaningful names by the researchers.

Table 1. Summary of e-business risks

e-business risk	Socio-technical component	Rationale
Unreliable technology	Technology	Uncertainty from e-business' critical reliance on immature technology, which is vulnerable to denial of service attacks, buggy software etc.
Lack of expertise in doing e-business	Actor-Technology	Uncertainty from the interaction of immature technology with inexperienced employees
Dependence on customers, suppliers, software vendors, the government etc.	Actor-Structure	Uncertainty from the interaction of e-business structure with (1) consumers' lack of acceptance; (2) government intervention e.g. taxes; and (3) supplier/vendor lack of cooperation
An inadequate e-business strategy	Actor-Structure	Uncertainty from the interaction of e-business structure with management who neglect strategic vision, goals and plans
Lack of profitability	Task-Actor	Uncertainty from the interaction of e-business tasks with management who sacrifice profitability for growth e.g. free or low pricing
Competitive issues	Actor-Structure	Uncertainty from the interaction of e-business structure with management who do not understand first mover advantage, switching costs, and complementarities
Leadership issues	Actor	Uncertainty from leadership lacking experience and too focused on technology
Reputation issues	Technology-Structure	Uncertainty from lack of alignment between technology and e-business workflow structure such as logistics
Legal issues	Technology-Structure	Uncertainty from lack of alignment between technology and authority such as government regulation e.g. HIPAA
Currency issues	Technology-Structure	Uncertainty from lack of alignment between e-business technology and currency conversion
Culture issues	Task-Actor	Uncertainty from lack of alignment between employees and tasks that would avoid cultural issues e.g. appropriate language
Intellectual property issues	Task-Structure	Uncertainty from lack of alignment between e-business structure and tasks that would avoid intellectual property issues e.g. downloading content

Table 1. (contd.)

e-business risk	Socio-technical component	Rationale
Identity issues	Task-Structure	Uncertainty from lack of alignment between e-business structure and tasks that would avoid identity issues e.g. smart cards
Identification issues	Task-Structure	Uncertainty from lack of alignment between e-business structure and tasks that would avoid identification issues e.g. digital signatures
Security issues	Task-Structure	Uncertainty from lack of alignment between e-business structure and tasks that would avoid security issues e.g. encryption
Privacy issues	Task-Structure	Uncertainty from lack of alignment between e-business structure and tasks that would avoid privacy issues e.g. sale of customer data

Following a review of the IS research risk literature and e-business articles, 16 e-business risks were identified. An online survey was designed to measure perceptions of each e-business risk. Respondents were asked to rate each risk on a seven point Likert scale ranging from "Extremely low risk" to "Extremely high risk". Demographic information was collected on job responsibilities, age, gender, experience in e-business, functional area and business role. A pretest of the survey was conducted with seven faculty in a Western U.S. business school. Input was requested on the time to complete and length of the questionnaire, clarity of the instructions and questions, and suggestions for additional questions or deletions. Based on the feedback received, modifications were made to the survey. A pilot study of the questionnaire with a class of 26 graduate students did not reveal any problems with administration or wording so no further modifications were necessary.

4 Data collection

Several sources were used to approach respondents. Email was used to send the URL of the online questionnaire to more than 12 organizations affiliated with a large Western U.S. university including mailing lists for alumni, a center for entrepreneurship and a group of business supporters of the university. Emails were also sent to professors in the business school asking them to post the URL for their graduate students. The majority of these graduate students attend classes at night and hold full-time jobs. Table 2 shows that the sample includes 194 respondents forming a diverse group of e-business providers and users.

5 Results

Respondents rated their perception of e-business risks from 1 (extremely low risk) to 7 (extremely high risk). See Tables 6, 7 and 8 for the survey questions

Table 2. Demographics of the study sample (N = 194)

e-Business providers and users		**Gender**	
Providers	14.30%	Male	60.70%
Users	36.20%	Female	37.20%
Both	16.80%	No response	2.00%
Neither	32.70%		
Age distribution		**e-Business experience**	
Under 20 years	1%	None	31%
20–25 years	12%	Less than 6 months	2%
26–30 years	30%	6–12 months	9%
31–35 years	17%	13–18 months	9%
36–40 years	13%	19–24 months	12%
41–45 years	9%	25–30 months	3%
46–50 years	6%	31–36 months	11%
Over 50 years	11%	37–42 months	3%
		43–48 months	5%
		49–54 months	3%
		55–60 months	4%
		More than 60 months	4%
Functional area		**Business role**	
Accounting	8%	Administrative staff	7%
Finance	5%	Consultant	18%
HR	5%	Executive	1%
Management	1%	Mgmt (entry level)	8%
Marketing	6%	Mgmt (mid-level)	17%
Purchasing	2%	Self-employed/partner	3%
Shipping	1%	Student	9%
Technology	39%	Support staff	16%
Non-computer technology	5%	Other	13%
Other	25%		

(reordered). The means of all the e-business risks, with the exception of "competitive" (2.45) are in the medium risk category, ranging from 3.42 for "legal" to 4.67 for "profitability" (See Table 3).

Standard deviations were reasonable varying from 1.326 for "competitive" to 1.748 for "identify". The top three perceived risks were profitability, privacy and security. While privacy and security are widely acknowledged e-business risks, profitability is more surprising as the number one concern. Leadership, expertise and reliability of technology were the next three concerns, showing that e-business has risks in common with business in general.

The impact of demographic variables was examined using one-way ANOVA for job responsibilities (e-business providers versus users), age distribution, business experience, functional area and business role and using a two-tailed t test for gender.

For most of the 16 risks, there is no significant difference in perception by e-business providers and users. However, one-way ANOVA shows there is a significant difference for privacy risk ($p = .021$) and competitive risk ($p = .015$). Not surprisingly, providers perceive privacy risk to be lower than users and other non-providers. Providers and respondents who classified them-

Table 3. Means and standard deviations of e-Business risk variables

	Mean	Std. Deviation
Profitability	4.67	1.549
Privacy	4.62	1.612
Security	4.59	1.522
Leadership	4.48	1.610
Expertise	4.22	1.703
Reliability	4.15	1.511
Identity	4.11	1.650
Culture	4.10	1.596
Reputation	4.06	1.668
Identify	4.03	1.748
Dependent	3.91	1.604
Strategy	3.64	1.501
Intellectual property	3.63	1.741
Currency	3.55	1.724
Legal	3.42	1.631
Competitive	2.45	1.326

selves as both providers and users perceive the risk from competition to be lower than users (and the group not participating in e-business) do.

A two-tailed t test was performed for each of the 16 risks to ascertain whether perception of risk varied by gender. No statistically significant difference was found for any of the 16 perceptions of risk.

Using one-way ANOVA there is no statistically significant difference for any of the risks by age, with the exception of ''identify'' ($p = .047$). Perception of risk was lowest for 26–30 years (mean 3.66) and highest for the 41–45 years age group (mean 5.31).

None of the 16 risks have a statistically significant difference by e-business experience using one-way ANOVA.

There is no statistically significant difference for any of the risks by functional area, with the exception of ''strategy'' ($p = .042$) using one-way ANOVA. Accounting perceives strategic risk lowest (mean 2.56) and shipping, HR and marketing highest (more than 4).

One-way ANOVA shows no statistically significant difference for perception of e-business risks by business role.

5.1 Factor analysis of the e-business risks

The exploratory factor analysis used SPSS, Extraction Method: Unweighted Least Squares and Rotation Method: Varimax with Kaiser Normalization. Three factors emerged with eigenvalues above 1 (6.157, 1.703, 1.305), explaining 57.3% of the variance. See Table 4. Overall reliability for the 16-item scale is .89. The loadings indicate high discriminant validity since all items except ''identify'' and ''legal'' load much higher on their relevant factor than the other two factors.

Factor 1 includes leadership, reliability, expertise, culture, reputation, currency, legal and profitability. Factor 2 consists of privacy/identity/

Table 4. e-Business risk factors

	1	2	3
Leadership	**.761**	.060	.244
Reliability	**.727**	.255	.154
Expertise	**.675**	.010	.370
Culture	**.657**	.218	.119
Reputation	**.573**	.309	.353
Currency	**.519**	.434	.073
Legal	**.491**	.478	.164
Profitability	**.381**	.214	.281
Privacy	.066	**.694**	.167
Identity	.172	**.693**	.170
Security	.125	**.672**	.144
Intellectual property	.406	**.545**	.052
Identify	.187	**.373**	.346
Strategy	.365	.167	**.606**
Competitive	.081	.144	**.554**
Dependent	.174	.096	**.530**
Eigenvalue	6.157	1.703	1.305
% variance explained	38.481	10.641	8.157
Cronbach alpha	.869	.782	.618

security/intellectual property/identify. Factor 3 consists of strategy/competitiveness/dependence.

The interpretation of the three factors follows. Factor 2 is typically associated with e-business more than traditional business and so the factor is called e-business "policy" risk. Risks such as privacy, security, and intellectual property and identity abuse loaded on this factor. Both practitioners and academics are well aware that these policy risks need attention and that the organization needs to construct policies that cover contingency plans, training and legal issues for example.

Although the other two factors are relevant for business in general, characteristics of e-business such as global reach and 24X7 availability exacerbate organizational and strategic risks. We name Factor 1 "socio-technical organizational". While all organizations need strong leadership and profitability, some pioneering e-businesses thought otherwise even when dependent on funding from venture capitalists or impatient investors. While all organizations that use technology need technical expertise and reliable technology, e-business is particularly vulnerable. The global reach of e-business accentuates the need to cope with a diversity of cultures and multiple currencies. The risk from a blemished reputation is applicable to all business, yet the Internet enables news to spread so quickly that reputations play a larger role in e-business.

The third factor is called "strategic stakeholder". Similarly to the other factors, e-business, having lower search costs and being externally focused, is particularly vulnerable to becoming less competitive, misalignment of strategic vision with the e-business, and too much dependence on vendors and other outsiders.

Cronbach's alpha results show significant correlation within each factor (.869 for organizational risks, .782 for policy risks and .618 for strategic

Table 5. Correlation of profitability and risks

Strategic risks		Organizational risks		Policy risks	
Strategy	.349	Reputation	.427	Security	.309
Competitive	.199	Reliability	.425	Privacy	.305
Dependent	.188	Leadership	.417	Identify	.295
		Culture	.333	Intellectual property	.238
		Expertise	.301	Identity	.173
		Currency	.290		
		Legal	.275		

risks). The corrected item-total correlation indicates the relationship between a given item and the other items. The range for corrected item-total correlation was .36 to .69 (.48 to .69 for organizational risks, .47 to .57 for policy risks and .36 to .57 for strategic risks).

Profitability is not as good a fit as an organizational risk as other items in this factor. An alternative interpretation is to consider profitability an outcome of risk management rather than a risk itself. In this case, correlations indicate that some organizational risks affect profitability more than strategic risks or policy risks. In particular, reputation, reliability of the technology and leadership have the highest correlation with profitability ($>.4$ and significant at the .01 level). See Table 5. This raises interesting implications for management.

6 Discussion

In this study, very few of the demographic variables influenced perception of e-business risks. This is not surprising given that the online population has become almost as diverse as the population in the United States. The sample, although not random, is diverse and reasonably representative of the online population.

Many of the 16 e-risks are significantly correlated. There are several inter-relationships. Reputation is affected by security breaches and privacy violations. Reliability of technology and reputation influence trust. Effective leadership resolves strategic and cultural issues.

Three factors emerged from the exploratory factor analysis. The factors are named strategic, organizational and policy risks. Strategic risks are associated with strategy, competitiveness, and becoming dependent. Survey respondents rated risks from extremely low to extremely high. See Tables 6, 7 and 8 for the questions used on the survey, grouped into the 3 factors (not the order of the questions on the survey).

Table 6. Strategic stakeholder risks

What is the risk that doing e-business will not accurately reflect the company's strategic vision?
What is the risk that conducting e-business will make the company less competitive?
What is the risk that in doing e-business the company will become dependent on others, such as personnel firms, consultants, or vendors?

Table 7. Socio-technical organizational Risks

What is the risk that the company management will be unable to provide adequate leadership for its e-business?
What is the risk that in doing e-business will tarnish the company's reputation because of poor customer service, unfilled orders, or delays?
What is the risk that the company's e-business technology will be unreliable?
What is the risk that there is insufficient technical expertise available to properly run the e-business technology?
What is the risk that the company's e-business will not operate profitably?
What is the risk that the company's e-business system will not comply with local, state, and federal, and/or foreign laws and regulations?
What is the risk that the company will not adequately adapt to other cultures, languages, etc., while conducting e-business?
What is the risk that the company will not be able to manage multiple currencies or exchange rates?

Strategic risks are those that concern upper management. Executives need to articulate the company's vision and monitor e-business compliance with the vision. Top management is also concerned with the organization's competitive position. Many organizations have found the cost of doing e-business is higher than they anticipated. To gain market share and become competitive, some companies have lowered prices. As a result many dot-coms and brick-and-click companies have found e-business extremely risky to organizational survival. Becoming dependent on vendors or other firms has aggravated the strategic risks. Dependency has often resulted in loss of control, although there may be no alternative if a core competency is not available in-house. In terms of the socio-technical model, strategic risks have an actor-structure component. The "actor" is a stakeholder who is either internal or external to the organization. Internal actors are management or other employees. External actors are customers, suppliers or vendors. Management with poorly conceived goals and false beliefs and values gave rise to risky e-business strategies.

Organizational risks are associated with leadership, reputation, culture, currency, reliability, expertise, legal issues and profitability. (See Table 7.)

Half of the 16 risks in this study load on the organizational risk factor. Some of these risks, such as inadequate leadership and reputation are not exclusive to e-business. Nevertheless, organizational risks need more attention from e-business, researchers and the media than they have given. Leadership was often neglected in the dot-com boom, when inexperienced

Table 8. Policy risks

What is the risk of security abuse, such as attacks by hackers?
What is the risk of privacy abuse, such as people reading your e-mail or making your personal information available to others
What is the risk that conducting e-business will place the company's intellectual property, such as trade secrets and patents, in jeopardy?
What is the risk of identification abuse, such as having one's identity stolen?
What is the risk of inaccurate business identification, meaning that people might not know with whom they are doing e-business?

technologists started companies. Reputations can be ruined more quickly online with the rapid spread of information. The enthusiasm to use e-business technology while it was immature and expertise was in short supply contributed to the downfall of some organizations. Profitability has been elusive for multiple reasons including the risks in this study. Non-compliance with local to international legal regulations has been another impediment to successful e-business. Finally, the global reach of e-business underscores the importance of attending to cultural diversity and currency issues. In terms of the socio-technical model, organizational risks have technology (reliability), actor-technology (expertise), actor (leadership), task-actor (culture, profitability), and technology-structure (reputation, legal, currency) components. Inappropriate actors for the task do not know how to manage cultural and profitability issues. Technology that is not aligned with workflow puts reputation and appropriate currency at risk. Technology that is not aligned with authority puts legal issues at risk.

Policy risks are associated with security, privacy, intellectual property, identity and identification. (See Table 8.) Security and privacy risks are especially well known in the context of e-business. As explained earlier in the paper, organizations need to adopt and document policies for security, privacy, intellectual property, identity and identification. Privacy policies are now usually posted on Internet sites. Identity theft, from posting customer social security numbers, credit card numbers or bank account numbers, are unlikely if adequate security and privacy policies are followed. Policies can also guard against abuse of intellectual property and fraud from inaccurate business identification. In terms of the socio-technical model, policy risks have a task-structure component. An inappropriate structure for the task generates out of control situations. Policies provide the control structure needed.

Using the three e-business factors and findings from prior research discussed earlier, we propose a model for control of e-business risks, shown in Fig. 2. Future research could test this proposed model. This model shows that use of control mechanisms generate trust and reduce perceived uncertainty, which in turn reduces perceived risks. Since a reduction in perceived risks would encourage e-business, it would also contribute to e-business profitability. The control mechanisms have been identified from the literature review. Some examples include a privacy policy for policy control, biometrics for technology control, HIPAA for legislation control, the Board of Directors for management control and a security audit for audit control. In many cases, control is relative rather than absolute.

E-business policy risks could be reduced using policy, technology and legislation control mechanisms to increase cognitive trust from consumers, who would perceive a reduction in uncertainty and hence lowered risk. Privacy policies, for example, tend to reassure consumers. E-business strategic risks could be reduced using management and audit control mechanisms. E-business organizational risks could be reduced using management control mechanisms.

Since our analysis showed significant correlation among many risks, it follows that controlled risks impact each other, as shown by the double-headed arrows. For example, if security (a policy risk) is well controlled then it is less likely that the website will be compromised which would threaten the firm's reputation (an organizational risk).

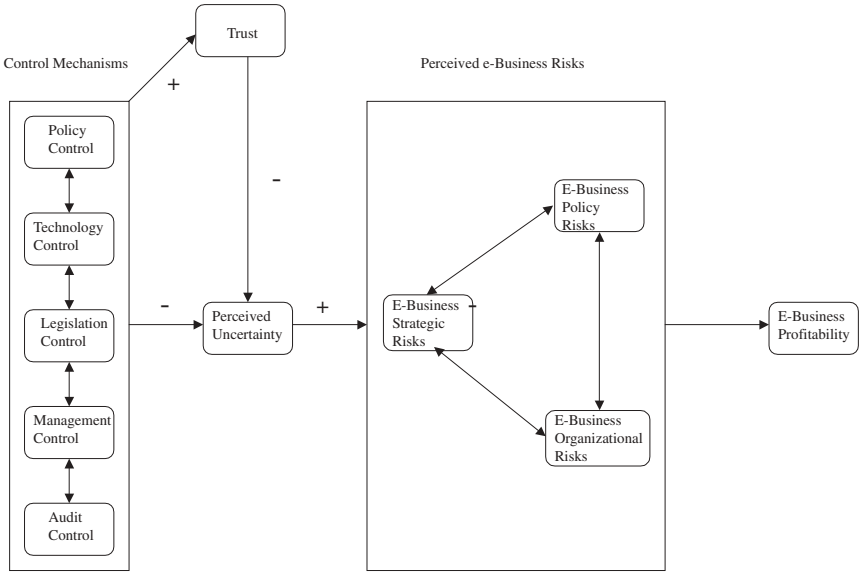

Fig. 2. A proposed model for control of e-business risks

7 Conclusion

Managing e-business risks is an important issue. Over the last few years, many start-ups have gone out of business largely due to mismanaging e-business risks and several traditional businesses have experienced negative consequences from mismanaging e-business risks. Also many consumers have avoided the Internet because of their fear of e-business risks. The impact on the global economy has been severe.

Prior research has given very little attention to perceived e-business risks apart from security and privacy. This study, using a socio-technical approach, identified sixteen e-business risks from a literature review of research and practitioner articles. Almost 200 respondents to a survey rated the severity of the e-business risks. Their top concerns were profitability, privacy and security. Three meaningful and logical e-business risk factors determined using exploratory factor analysis were strategic, organizational and policy risks. In terms of the socio-technical model, strategic risks focus on the actor-structure component, and policy risks focus on the task-structure component. Organizational risks cover a wide spectrum of socio-technical components such as technology, actor-technology, technology structure and task-actor. The main contribution of this study is a multi dimensional scale of perceived e-business risks. A further contribution is a model proposed for testing in future research. The model incorporates the three dimensions of e-business risks and shows theoretically based relationships with control mechanisms, trust, perceived uncertainty and profitability.

7.1 Implications for management

Management has become more aware of e-business risks since the dot-com crash of 2000. The lessons to be learned include identifying e-business risks and using control mechanisms to manage risks and increase the likelihood of business viability. This study raises the awareness of management to three risk factors. While e-business risks associated with security, privacy and other policies have garnered most of the attention, this study shows that profitability is the top concern and traditional organizational and strategic risks are critical and should not be ignored. During the years of exuberance, organizational and strategic risk factors, such as leadership and culture, were often overlooked. However, global reach, 24X7 availability and other characteristics of e-business exacerbate organizational and strategic risks, and history and the results of this study have reaffirmed their relevance.

7.2 Implications for research

Several responses to an ISWorld survey of researchers on important issues in e-commerce included security and privacy (Benbasat et al. 2000). Similarly, another source emphasizes that research needs ''to understand the efficacy of government regulations that ensure privacy and digital security in such sensitive industry sectors as financial services and healthcare, .. in various settings on the Internet'' (Kauffman and Walden 2001). Although security and privacy are critical, this study examines a more comprehensive list of risks, raises awareness of other e-business risks and builds on prior research on risks in other information technology contexts. In this way it continues the cumulative tradition, which is highly valued in the field of IT research. Specifically, this study extends prior socio-technical research on information technology related risks in systems development to the context of e-business.

The main contribution of this study is a multi dimensional scale of perceived e-business risks. A limitation of this study is the exploratory nature of the factor analysis. However, this methodology is appropriate given the immaturity of this area of research. Future research should explore other e-business risk variables and apply confirmatory factor analysis to the three factors derived in this study. Confirmatory factor analysis will bring more rigor to the findings and will enable further progress towards establishing a measuring instrument for perceived e-business risks. A measuring instrument could be used for benchmarking organizations in terms of their e-business risks. Another avenue is to find empirical support for our proposed model using structural equation modeling, for example. Implicit in the model are research questions such as: Which control mechanisms are most effective and under what conditions? What is the relationship among the control mechanisms? Which risks respond to which control mechanism?

Research on perceived e-business risk is important because the severe consequences of neglecting risk. Organizations need to use control mechanisms to manage e-business risk, to avoid failure and also to leverage opportunities. Consumers need to manage e-business risk to become satisfied online customers who will contribute to the global economy.

Acknowledgement. The author would like to thank David E. Griggs and Robert W. Simmons, who as graduate students assisted with the data collection. Thanks to the reviewers and Professors Peter Bryant and Elizabeth Cooperman for their suggestions on how to improve the paper.

References

Alavi M, Weiss IR (1985/1986) Managing the Risks Associated with End-User Computing. *Journal of Management Information Systems*, 2(3): 5–21

Amit R, Zott C (2001) Value Creation in e-Business. *Strategic Management Journal*, 22(6/7): 493–520

Anestopoulou M (2001) Challenging Intellectual Property Law in the Internet: An Overview of the Legal Implications of the MP3 Technology. *Information & Communications Technology Law,* 10(3): 319–337

Bagozzi RP (1981) An examination of the validity of two measures of attitude. *Multivariate Behavioral Research*, 16: 323–359

Barki H, Rivard S, Talbot J (1993) Toward an assessment of software development risk. *Journal of Management Information Systems,* 10(2): 203–225

Barki H, Rivard S, Talbot J (2001) An Integrative Contingency Model of Software Project Risk Management. *Journal of Management Information Systems*, 17(4): 37–70

Beard A, Ehrenreich J (2000) Cybercrime: Arms Race in a New Space. *Risky Business*, 1, PriceWaterhouseCoopers

Benbasat I, Ives B, Piccoli G, Weber R (2000) E-commerce top questions. *ISWorld.* http://www.commerce.uq.edu.au/isworld/research/msg.22-02-2000-1.html

Berghel H (2000) Identity theft, social security numbers, and the Web. *Communications of the ACM*, (February) 43(2): 17–21

Bollen KA (1989) *Structural Equations with Latent Variables.* Wiley Interscience

Boyd J (2001) Airport Security May Get Smarter. *Internet Week*, http://www.internetweek.com/story/INW20011206S0004

Camp LJ (1999) Web Security and Privacy: An American Perspective. *The Information Society,* 15(4): 249–256

Computer Emergency Response Team (CERT) (2002) CERT Statistics. *CERT*, http://www.cert.org/stats/cert_stats.html

Computerworld (2001) Security Statistics. *Computerworld,* http://www.computerworld.com/2001/0,4814,62002,00.html

Clarke R (1999) Internet privacy concerns confirm the case for intervention. *Communications of the ACM***,** 42(2): 60–67

Clemons EK, Thatcher ME, Row MC (1995) Identifying sources of reengineering failures: A study of the behavioral factors contributing to reengineering risks. *Journal of Management Information Systems,* 12(2): 9–36

Cranor LF (1999) Internet privacy. *Communications of the ACM,* 42(2): 29–31

Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science*, 10: 104–115

Cunningham S (1967) The Major Dimensions of Perceived Risk. In: Cox D (ed) *Risk Taking and Information Handling in Consumer Behavior*, Harvard University Press, Cambridge, Mass

Dean R, Carey A (2000) Executive Insights on Content Security: Proactively Addressing Potential Liabilities in the New Economy, IDC, *Computerworld*

De Figueriedo JM (2000) Finding Sustainable Profitability in Electronic Commerce. *Sloan Management Review*, 41(4): 41–52

Dekleva S (2000) Electronic Commerce: A Half-Empty Glass? *Communications of AIS*, 3(18): 1–99

De Lotto R (2001) Clickstream: Fine to Track Customers; Best at Losing Them**,** *Gartner Research Note Strategic Planning Assumption*

Duffy D (2000) Special Security Report: Cyberinsurance Prepare for the worst. *Darwin Magazine*, http://www.darwinmag.com/read/120100/worst.html

Ernst and Young (2001) Information Security Survey 2001. *Ernst and Young Information Systems Assurance and Advisory Services*
Ettredge M, Richardson VJ (2001) Assessing the Risk in E-Commerce. *Proceedings of the 22nd International Conference on Information Systems*, New Orleans, 275–284
Freedman DH (2002) What eBay Isn't Telling You. *Business* 2.0: 57–61
Gefen D (2002) Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers. *DataBase*, 38–53
Ghosh AK, Swaminatha TM (2001) Software security and privacy risks in mobile e-commerce. *Communications of the ACM*, 44(2): 51–57
Hinde S (2002) 2001: A Privacy Odyssey Revisited. *Computers & Security,* 21(1): 16–34
Hine C, Eve J (1998) Privacy in the Marketplace. *The Information Society*, 14(4): 253–262
Hoffman DL, Novak TP, Peralta M (1999) Building consumer trust online. *Communications of the ACM*, 42(4): 80–85
Hunter R (2002) Security Section 01 You Can't Hide. *Gartner* http://security1.gartner.com/event.php.id.2.jsp
Huston T (2001) Security issues for implementation of e-medical records. *Communications of the ACM*, 44(9): 89–94
Iwata E (2000) E-commerce losses drive dot-com insurance. *USA Today*, http://www.usatoday.com/life/cyber/tech/cth339.htm
Kaihla P (2001) Five Battle-Tested Rules of Online Retail. *e Company,* 2(3)
Kauffman RJ, Walden EA (2001) Economics and Electronic Commerce: Survey and Directions for Research. *International Journal of Electronic Commerce*, 5(4): 5–116
Keil M, Cule PE, Lyytinen K, Schmidt, RC (1998) A Framework for Identifying Software Project Risks. *Communications of the ACM*, 41(11): 76–83
Kern T, Willcocks LP, Lacity MC (2002) Application Service Provision: Risk Assessment and Mitigation. *MIS Quarterly Executive*, 1(2): 113–126
King WR, Teo TSH (1996) Key Dimensions of Facilitators and Inhibitors for the Strategic Use of Information Technology. *Journal of Management Information Systems*, 12(4): 35–53
Lord G et al. (2001) New Strategies for Success in E-Business: Managing Risks to Protect Brand, Retain Customers, and Enhance Market Capitalization. *KPMG International*, http://www.us.kpmg.com/RutUS_prod/Documents/12/espace1.pdf
Lemke T (2002) Internet Attacks Reported on the Rise. *eCommerce Times*, http://www.ecommercetimes.com/perl/story/18495.html
Lyytinen K, Mathiassen L, Ropponen J (1998) Attention Shaping and Software Risk - A Categorical Analysis of Four Classical Risk Management Approaches. *Information Systems Research*, 9(3): 233–255
M2 Presswire (2000) International Credit Card Fraud. *Nationalfraud.com*, http://www.nationalfraud.com/stats.htm
McAllister DJ (1995) Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, 38(1): 24–60
Milberg SJ, Smith HJ, Burke SJ (2000) Information Privacy: Corporate Management and National Regulation. *Organization Science*, 11(1): 35–57
Mitchener J (2000) Extended Communities for Future E-Business. *Internet Society INET Proceedings*, http://www.isoc.org/inet2000/cdproceedings/7b/7b_1.htm
Moscove SA (2001) E-Business Security and Controls. *CPA Journal*, 71(11): 40–44
Nidumolu SR (1996) A comparison of the structural contingency and risk-based perspectives on coordination in software development projects. *Journal of Management Information Systems*, 13(2): 77–110
Oppliger R (1997) Internet Security: Firewalls and Beyond, *Communications of the ACM*, (May) 40(5): 92–102
Palmer JW, Bailey JP, Faraj S (2000) The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements. *Journal of Computer-Mediated Communication* [On-line], 5(3) http://www.ascusc.org/jcmc/vol5/issue3/palmer.html
Patient S (2000) Caveat Vendor: Reducing Online Credit Card Fraud, http://www.webdevelopersjournal.com/articles/card_fraud.html

Pescatore J (2002) Technology of Survival, Security Section 03. *Gartner*, http://security1.gartner.com/event.php.id.5.jsp
Porter M (2001) Strategy and the Internet. *Harvard Business Review*, 79(3): 63–78
Potter C (2000) E-Business Risk Management: Risks on the Virtual Frontier. *Risky Business,* 1, PriceWaterHouseCoopers http://www.pwcglobal.com/extweb/pwcpublications.nsf/docid/D3D286020690839B80256A0F003B64F1
Radcliff D (2001) Calculating E-Risk. *Computerworld*, http://www.computerworld.com/storyba/0,4125,NAV47_STO57529,00.html
Reagle J, Cranor LF (1999) The platform for privacy preferences. *Communications of the ACM,* 42(2): 48–55
Regan K (2002) The E-Commerce Tax Bottom Line. *E-Commerce Times*, http://www.ecommercetimes.com/perl/story/17447.html
Resnick P, Zeckhauser R, Friedman E, Kuwabara K (2000) Reputation systems. *Communications of the ACM*, 43(12): 45–48
Rose G, Khoo H, Straub DW (1999) Current technological impediments to business-to-consumer electronic commerce. *Communications of the AIS,* 1(16): 1–4
Saban KA (2001) Strategic Preparedness: A Critical Requirement to Maximize E-commerce Investments. *Electronic Markets*, 11(1): 26–36
Sabo D (1998) Electronic Commerce Barriers Survey Results. *Information Technology Association of America*, http://www.itaa.org/software/research/indpulse/bartext.htm
Sager I (2000) Cyber Crime. *BusinessWeek Online*, http://www.businessweek.com/2000/00_08/b3669001.htm
Salkever A (2002) Special Report: The Security Challenge, Cybersecurity's Leaky Dikes. *BusinessWeek Online*, http://www.businessweek.com/technology/content/jul2002/tc2002072_9216.htm
Schlarman S (2002) The case for a security information system. *Information Systems Security,* 11(1): 44–50
Schmidt R, Lyytinen K, Keil M, Cule P (2001) Identifying Software Project Risks: An International Delphi Study. *Journal of Management Information Systems*, 17(4): 5–36
Scott JE, Vessey I (2002) Managing Risks in Enterprise Systems Implementations. *Communications of the ACM*, pp 74–81
Shneiderman B (2000) Designing Trust into Online Experiences. *Communications of the ACM*, 43(12): 57–59
Smith HA, McKeen JD, Staples DS (2001) Risk Management in Information Systems: Problems and Potential. *Communications of the AIS*, 7(13): 1–29
Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2): 167–196
Straub DW, Welke RJ (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 21(3): 441–469
Straub DW, Watson RT (2001) Research Commentary: Transformational Issues in Researching IS and Net-Enabled Organizations. *Information Systems Research*, 12(4): 337–345
Stewart KA, Segars AH (2002) An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1): 36–49
Tan Y, Thoen W (2000) A Logical Model of Trust in Electronic Commerce. *Electronic Markets*, 10(4): 258–263
Van Mien AD (2000) E-Business Raises Transaction Security Concerns. *Gartner Research Note*
Wang H, Lee MKO, Wang C (1998) Consumer Privacy Concerns about Internet Marketing. *Communications of the ACM*, 41(3): 63–70
Weil P, Ross J, Vitale M, Straub D (2001) E-Business Autopsy: What Have We Learned? Panel *Twenty-Second International Conference on Information Systems*, (December 19), http://web.mit.edu/cisr/www/html/icis.html
Willcocks LP, Lacity MC, Kern T (1999) Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA. *Journal of Strategic Information Systems*, 8: 285–314

Willcocks LP, Griffiths C (1997) Management and Risk in Major Information Technology Projects. In: Willcocks LP, Feeny D, Islel G (eds) *Managing IT as a Strategic Resource*, McGraw-Hill, Berkshire England, pp 203–237

Zacharia G, Moukas A, Maes P (2000) Collaborative Reputation Mechanisms for Online Marketplaces. *Decision Support Systems*, 29: 371–388