E commerce

Business, E-Commerce

Information risks stem from information published and contained In web sites and associated with the conduct of e- amerce. Peripheral to Information risks are risks associated with misuse of information, such as violation of laws in the united States and other countries. Technology risks include risks involving hardware, software, telecommunications and databases. These risks include the consequences resulting from the misuse of technology or the use of inappropriate technologies required to address business needs.

Business risks concern customer and supplier relationships, and risks associated with products and services marketed and distributed over the Internet. They also Include risks associated with managerial aspects of the business Including response and contractual relations. Because e-commerce straddles many functional and technical areas, authors in many disciplines have identified e-commerce-related risks. Examples of these can be found in [1], and [6].

From these sources and from the general risk management literature for example, [8] we compiled a partial list of risks that appears below. 1. Information Risk Content on web page exposing web publisher to libel, defamation of character, slander 1. 2. Copyright infringement and invasion of privacy suits stemming from posted textual content 1. 3. Copyright infringement and invasion f privacy suits stemming from digital scanning and morphing 1. 4. Copyright, patent, or trade secret infringement violations by material used by web site developers 1. 5.

After unauthorized access to a web site, online Information about employees or customers Is stolen, damaged or released without authorization Electronic bulletin boards containing defamatory statements resulting In liability or embarrassment 1. 7. Worldwide legal exposure resulting from use of creative material (e. G. Names, likenesses) that violate laws of countries outside of the home country 1. 8. Credit card information intercepted in transit is disclosed or seed for fraudulent purposes 1. 9. Information that has been changed or inserted In transmission Is processed leading to erroneous results 1. 0. Flight of Intellectual property due to employees moving to competitors 2. Technology Risk Negligent errors or omissions in software design 2. 2. 2. 1. Access to a web site, unauthorized 2. 3. 2. 4. 2. 5. Infecting a web site with computer viruses Internet service provider (ISP) server crashes Software error and omission risks causing unauthorized access 2. 6. Intercepts credit card information in transit causing breeches in security for online Intercepting and copying or changing non-credit card aments. 2. 8. Information during transmission 2. 9.

Insufficient bandwidth to handle traffic 2. 10. Obsolete hardware or hardware lacking the capacity to process required traffic 2. 11. Risk due to excessive ISP outages or poor performance 2. 12. ISP phone numbers being busy 2. 13. ISP or home-company servers being down 2. 14. Scant technical infrastructure to manage cycle time to develop, present, and process web-based products 2. 15. Risk of improperly integrating e-commerce system with internal databases 2. 16. Risk of improperly integrating e-commerce system with internal operational processes 2. 7.

Risk due to poor web site design manifesting themselves in long response times 2. 18. Inability of customer or supplier computers to handle graphical downloads 3. Business Risk Web page content exposes web publisher to libel, defamation of character, 3. 1. Slander 3. 2. Electronic bulletin boards containing defamatory statements resulting in liability 3. 3. Information in violation of home-country laws 3. 4. Using web sites to conduct illegal promotional games, such as a sweepstakes or contests 3. 5. Risks related to payment to web site developers and disputes between developers and clients 3. Lack of maintenance on existing web pages Impact on business due to intellectual property lost due to employees 3. 7. Changes in supplier relationships re: data access, moving to competitors 3. 8. Data ownership, distribution strategy, and marketing tactics 3. 9. Changes in customer relationships re: data access, data ownership, distribution strategy, and marketing tactics 3. 10. Products out-of-stock due to poor communication with operations 3. 11 . High shipping costs required for distribution 3. 12. Inconvenient return policies lack of coordination with physical system 3. 13.

Excessive dependence on ISP to support firm's business strategy 3. 14. Inability to manage cycle time for developing, presenting, and processing web-based products 3. 15. Risk due to unprotected domain names which are usurped by other organizations 3. 16. Improperly integrating e-commerce systems with internal operational processes 3. 17. Insufficient integration of e-commerce with supply chain channels The above risks can lead to events resulting in the deliberate or inadvertent loss of assets. Deliberate loss of assets can result from disclosing information, fraud, or deliberate disruption of service.

Inadvertent loss of assets can occur through inadvertent disruption of service, legal penalties due to disclosure of information, or direct or indirect losses due to lost business. As losses of these forms can occur in non-e-commerce environments, what are the similarities and differences between e- commerce and non-e-commerce risk environments? RISK COMPARISON To compare risks in electronic and non-e-commerce risks we postulate three risk categories: Category A: Those risks that are essentially the same in either web page essentially is the same as legal liability due to information disseminated by rented or other electronic media.

Category B: Those risks that are essentially the same but that have unique dimensions dictated by e-commerce. For example, insufficient integration of e-commerce with supply chains might be an example of this risk. Category C: Risks that are unique to e-commerce and which have never appeared before in other environments. Analyzing the risks enumerated in the last section, yields a preponderance of risks falling in Category A. For example, our analysis, albeit subjective, indicates that all the Information risks risks 1. 1 through 1. 0, Technology Risks 2. 1 through 2. 4, and Business Risks 3. 1 through 3. 14 all fall in this category. We conclude this because these risks although they occur in e- commerce essentially are the same risks that occur in other environments and have been managed in those environments. There are several risks that we classify in Category B: Technology Risks 2. 15 through 2. 18 and Business Risks 3. 15 through 3. 17. For these, we conclude that although the risks are similar, the e- commerce environment is different enough to require unique treatment.

We found no risks in Category C risks unique to e-commerce and not encountered elsewhere. Even those things that appear to be unique for example illegal use off domain name or risks associated with Sips have counterparts in use of logos or corporate names, and risks associated with organizations contracted for outsourcing data processing. Naturally we do not imply that the above list of risks exhaust all possibilities certainly some may exist that fall in our Category B or even Category C.

We do believe, however, that the majority of risks encountered in e-commerce environments have been encountered before and generally, are well understood if identified. Can there be unique risks in electronic environments and if so, what re they? Although we have not identified any such risks here, we posit that they: 1) concern business issues that are unique to e-commerce and that are not found elsewhere; 2) involve technological attributes unique to e-commerce environments with no parallel issues found elsewhere; 3) impact risk in ways uniquely determined by characteristics of e-commerce.

Critical to managing e-commerce risks is a methodology that provides managers with the capability to identify, assess and control risks on an ongoing basis. One proposed methodology that does this is a scenario-based methodology patterned on Information Security Management Planning (ISMS), a methodology implemented at a large money center bank to control information-based risks [7]. METHODOLOGY TO MANAGE RISK Our methodology, E-commerce Risk Management (ECRU), is based on scenario analysis and decision analysis, but differs from these techniques in several ways.

First, by integrating business, operations, and systems managers into the risk analysis process, ECRU increases non-technical managers' ownership of the process and of the information-based risk issues. Second, ECRU is flexible enough to address issues specific to unique processing, geographic and organizational environments. Third, ECRU can be implemented at relatively low cost. ECRU can identify potential risk events in their early stages and by preventing their occurrence, lead to lower risk management costs.

The actual risk management process consists of three The Preliminary Risk Assessment (PRAY) is a structured meeting between senior business, operations, marketing and systems managers. The Para's purpose is to highlight for further analysis, the key risk issues and areas facing the business unit. E-commerce risk is categorized in terms of risk target (where the risk occurs) and risk- type (Information Risk, Technology Risk, or Business Risk). The PRAY focuses on outcomes based on errors, omissions, structural weaknesses, and deliberate acts.

The resulting grid generates " target-risk combinations". The risk assessment involves the senior business manager's providing a risk rating for each target- outcome combination, given existing controls. Highly rated risks (on a 1-5 scale) include an explanation for why the rating was applied. Detailed Risk Assessment In the Detailed Risk Assessment (DRAG) the project team develops detailed risk scenarios for each highly rated PRAY target-outcome combination. The bases for the DRAG are scenarios based on the risks enumerated in above section.

The DRAG procedure is sequential includes: 0 Meetings with managers from target areas to gain insights regarding risk scenarios; Brainstorming sessions and follow-up reviews to identify potential scenarios; Rating the scenarios regarding risk on a 1 to 5 scale; Identifying potential controls; Selecting controls to be implemented. In this process, DRAG risk ratings need not reflect the PRAY target-risk combination rating. Cursory cost-benefit analysis often is sufficient to select or discard controls. Formal decision analysis is usually unnecessary and may be problematic.

The Drag's final step occurs when senior department and division managers review the scenarios and preliminary recommendations for final approval Controls Implementation In Controls Implementation the senior managers who participated in the PRAY review the study findings and recommendations. Recommended controls frequently close security gaps for " high risk" scenarios, reduce risk exposure at minimal cost, or scrap obsolete controls which are holdovers from previous years and now address non-existent risks. Actually implementing the recommended controls is the methodology's final phase.