

Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2002 Proceedings

International Conference on Electronic Business
(ICEB)

Winter 12-10-2002

Applying Business Models for Risk Management in E-Business

Andrew Finegan

Follow this and additional works at: <https://aisel.aisnet.org/iceb2002>

This material is brought to you by the International Conference on Electronic Business (ICEB) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICEB 2002 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Applying Business Models for Risk Management in E-Business

Andrew Finegan
School of Business Information Technology
RMIT University
Melbourne, Australia
andrew.finegan@rmit.edu.au

Abstract

This paper presents a case study of the application of business models for managing risk in the development of operational strategies for e-business. It includes issues of security, transaction protection, customer relationships, and data and content ownership. The investment that an e-business project is willing to make in risk management activities depends on the business model adopted, the experience of the project team, and the constraints imposed on both. This is particularly important when planning to use technology to do business in the global economy.

1. Introduction

In this paper e-business models, e-business development and operation strategies are examined within the framework of project risk management. A case study of a practical approach to project risk management is used to illustrate a specific project development strategy available to organisations working within the e-business environment.

2. Defining Project Risk

Project risk management is the practice of identifying, assigning, and responding to risk throughout the life of a project and with the goal of meeting project objectives [8, p.302]. Risk management can improve the process of selecting projects, determining the scope of project, and developing schedules and cost estimates. It assists project stakeholders understand the nature of the project, and encourages integration of the other project management knowledge areas.

Risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning [3, p.172]. A project must balance the possible negative consequences of risk against the potential benefits of its associated opportunity. In many respects, risk management is similar to insurance. Schwalbe [8, p.303] defines it as an activity undertaken to lessen the impact of potentially adverse events on a project. Like insurance, risk management is an investment with associated costs. The level of this investment is dependent upon the nature of the project, the experience of the project team, and the constraints imposed on both.

Why do organisations continue to undertake e-business projects if they are subject to risk and may cause loss or injury? Schwalbe [8, pp.303-304] observes that many companies are in business today because they took

risks that created great opportunities. Organisations survive over the long term when they pursue opportunities based upon innovation [5]. E-business may now be a key part of a business's strategy; without it many businesses might not survive. However, Greenstein and Feinman [3, p. 172] warn "*In the rush to deploy client/server and Web-related technologies and perhaps gain competitive advantage or generate higher revenue along the way few companies stop to consider that these systems may expose them to some operational and financial risks*".

3. E-Business and Risk

Faced with the necessity to engage in new forms for business based upon information technology, organisations are finding that there are two major e-business risk issues - security and the protection of transactions. In addition, these organisations must also consider the potential difficulties that they may have in adopting e-business technology and the specific threats that e-business present to the organisations.

3.1 Security

Currently, the major barrier to e-business is the consumer's lack of confidence in Internet security [7, p.158]. For e-business to be trustworthy, it must be secure and reliable. Users must feel confident when revealing sensitive information like credit card details that this information will be kept safe and secure.

Security is a constant consideration of any network-based application. It must address the following issues while still providing users access to the information:

- Authentication,
- Access control,
- Firewalls, and
- Encryption.

Firewalls are a combination of software and hardware, which manage access between a company's internal system and the Internet [3, pp.158-159]. A firewall allows a network administrator to determine which services and types of information are accessible through your Internet connection. Firewalls must be used in conjunction with an overall security policy to be most effective.

Encryption can be used after data has left an internal system. Encryption renders the data unreadable by using a mathematical formula known as a key. The data is turned back into readable form, i.e. deciphered, by

applying the correct key. Secure payment systems that people trust are pivotal to the continued growth of e-business. New payment systems like digital checks and electronic wallets are currently being developed, but credit cards are still the most common form of payment [7, p.239]. To set up a credit card payment system on your web site you need:

- An acquiring bank that will establish an Internet merchant account
- Payment processing software to transfer the credit card details between your bank and web site
- A secure certificate for data encryption

The most common encryption protocol in current use is SSL (Secure Sockets Layer) that was developed by Netscape [6]. SET (Secure Electronic Transactions) sponsored by Visa and MasterCard is another encryption technology, which is a new standard to enable secure credit card transactions on the Internet [9].

However, Greenstein and Feinman [3, p.158] and Schneider and Perry [7, p. 162] emphasise that effective Internet security requires policy as well as technology. A good security policy will ensure:

- Safety - that sensitive information sent across the Internet is protected during transit
- Trust - that information reaches its destination without tampering
- Privacy - that personal information stored is available only to authorised personnel

Questions to ask when developing your policy include:

- Who needs to have Internet and e-mail access?
- Do staff check email and fax numbers before sending confidential information?
- Are sensitive documents encrypted before being transmitted?
- Are parts of your internal computer system restricted?
- What do you do when employees leave? Do you have a password policy?

Security is about an approach to information management. In particular, protection of confidential client information is going to become more important as companies gather more information about clients through doing business on the Internet.

3.2 Protection of Transactions

In any e-business Weill and Vitale [10, pp.315-317] argue that the important question is “Who owns the transaction?” Organisations owning the customer transaction are able to set a fee or collect a profit margin for the service provided. The service could be for the sale of products, the provision of information or advice, or the provision of a professional service. Therefore, owning the customer transaction has the potential to generate customer revenue for the service. Owning the transaction also implies that the organisation owns the customer data related to those transactions. However, perhaps no other customer data will be owned unless the organisation also

owns the customer relationship. Owning the customer relationship provides influence where the customer looks to the relationship holder for trust, recommendations, and specialist advice.

The strength of the relationship with the customer will often determine the success of the business. The relationship will be determined by the strength the value of the service to the customer and the ability to deliver. This strength of will involve the brand, the breadth of offerings, the price-value equation, and the completeness of the consolidation into a single point of contact. Information is the lifeblood of e-business. The viability of many businesses will depend on access to information about customers' products, markets, and costs. The organisations ability to identify, capture, share, and exploit the key information strongly influences business profitability [10, pp.259-261].

Content providers are organisations that create and provide information products or services in digital form to be used by customers via third parties. In general the content provider owns none of the end-customer relationship, transaction, or data. Therefore, to be successful the content provider must be highly desirable and in demand as a supplier of content. Furthermore, not owning any of the customer assets - relationship, data, or transaction - makes the content provider very reliant on third parties. On the other hand, content providers typically have a relatively small number of direct customers, and therefore they do not incur the costs of managing relationships with a large number of customers [10, pp.253-256].

3.3 Potential difficulties

Many traditional and profitable businesses are challenged by the need to respond to the threats and opportunities of e-business.

Most large traditional firms are successful and profitable, and they achieved their success via strong leadership and cultures suited to their industry. Weill and Vitale [10, p.13] argue that these leaders are often poorly prepared to make major strategic commitments necessary for e-business, and are reluctant to take the initiative, preferring to wait and see. This attitude actively works against new initiatives that threaten the status quo. The challenge is that senior management must actively work to shape the e-business vision, their employees, and the organisational culture into a new model for the way business is undertaken.

Channel conflict is a real risk with e-business. The Internet offers a new channel to the customer, and businesses can choose to bypass existing channel partners, leading to channel conflict. Particularly difficult to handle is channel conflict where the customer is offered very similar value propositions directly, and alternatively by an intermediary, but at different prices. Steps to help avoid channel conflict include [10, pp. 306-307]:

- Segment the channels by customer by targeting the customers for online selling.

- Segment the channels by product by distributing some products online, and other products via traditional channels.
- Refine the dealers' role by defining the role of the retailer as one of display, test-drive, and configure the product or service.
- Develop a new brand or re-badge the existing product to sell directly, giving these items a different value proposition to the products sold by the retailers.
- Establish an information Web site with product description, and perhaps a virtual community, and pass all leads to the retail channel (the distributors).
- Retreat from selling similar products, and avoid an un-winnable price war.

Weill and Vitale [10, p.15] also argue that infrastructure requirements for e-business are stretching the capabilities of many organisations' IT portfolios. Traditional organisations are struggling with B2B e-business implementations that may require integrating their recently installed and expensive enterprise resource planning systems (ERPs) with their Web sites and the Web sites of partner firms. Also, one of the major challenges for the direct-to-customer organisation selling a physical product is getting the right product to the right address, reliably and economically. Many innovative businesses have developed attractive Web sites, but have not developed a clear understanding of the complex logistics involved in e-business. In response, some logistics companies see delivery of goods ordered via e-business as an opportunity to expand their influence (FedEx).

The use of multiple business models across an organisation can cause confusion for customers, especially if the customer needs to adopt a variety of different business practices within the organisation. Where various business units within the organisation use different models, confusion can arise if the customer is treated as a different entity by each business unit. Furthermore, implementing more than one model can lead to the further problems described above, including channel conflict, competency conflict, infrastructure conflict, and information conflict [10, p.82].

3.4 Threats from e-business

Organisations must also consider the specific threats that e-business make to the continued successful conduct of business. A number of questions should be addressed.

How large is the potential for competitors to undermine the loyalty of the organisation's customers? Weill and Vitale [10, p.294] observe that loyalty has two important components - brand identification, and switching costs. If customers have high brand identification, based on lifestyles and other personal traits, they will be more loyal. If the switching cost for a

customer to change brands is high, then they will also be more loyal.

How large is the gap between the current and the potential customer self-service?

Customer self-service is defined as providing an attractive value alternative to customers who can serve themselves. An important question asked by Weill and Vitale [10, pp.294-295] is: "*How much does your customer dislike dealing with your organisation in person.*"

What is the difference between your organisations current geographical reach and its potential reach with the Internet? Weill and Vitale [10, p.295] observe that the larger the gap, the greater the threat or opportunity from e-business. However, many organisations' geographical reach is limited by external constraints, including other countries' regulations, tariffs and *the* cost of transportation.

4. Case Study - *Razoredge Limited*

The following is a case study that is based upon a real world organisation - *RazorEdge Limited*. It illustrates a particular project approach to e-business development with attention to risk management issues.

The case is of an Australian buying group for retail business with the following profile:

- 700 Members (independent retailers) located throughout Australia.
- 500 Suppliers (manufacturers and/or importers).
- Au\$150 Million annual turnover.
- Gross profit margin is 2.5 - 3.5% (very lean!!!).
- 55 Suppliers use electronic data interchange (EDI)
- These suppliers contribute 65% to 75% of business.
- 70% of members have access to a computer.
- Employs about 40 staff in two groups - Marketing, and Finance and Management.

The major challenge faced by *RazorEdge Limited* is the fear that suppliers or others will use technology to exclude the company from the loop. Also, business models are changing, as are relationships due to technology. Specifically *RazorEdge Limited* seeks to achieve the following objectives:

- Greater efficiencies and reduction in costs.
- Better communication with our members, suppliers, and the wider industry.
- Form alliances with key suppliers without risking loss of business, especially direct trading between suppliers and members.
- Increase revenue through special products, supplier links, and bulk order taking.
- The new bottom line - "Branding" is essential - *RazorEdge Limited* - the business and the brand must be leaders in the market, both "real" and "electronic".

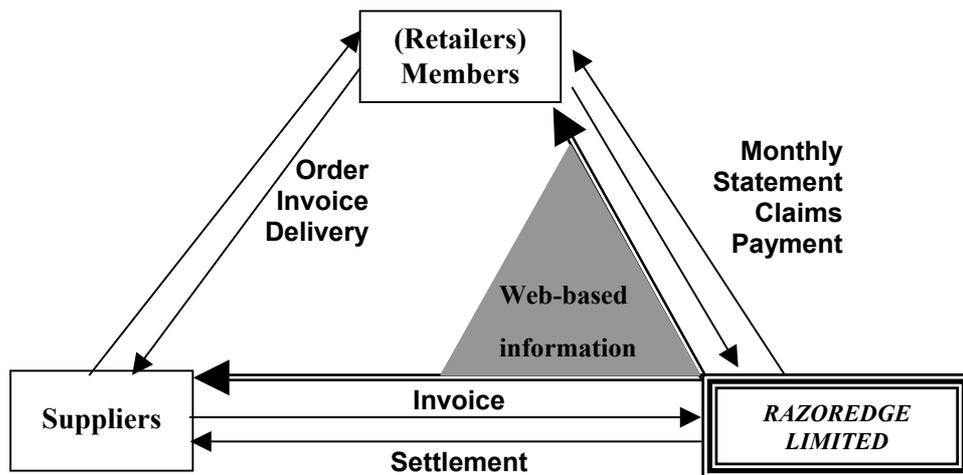


Figure 1 - *RazorEdge Limited* current business model

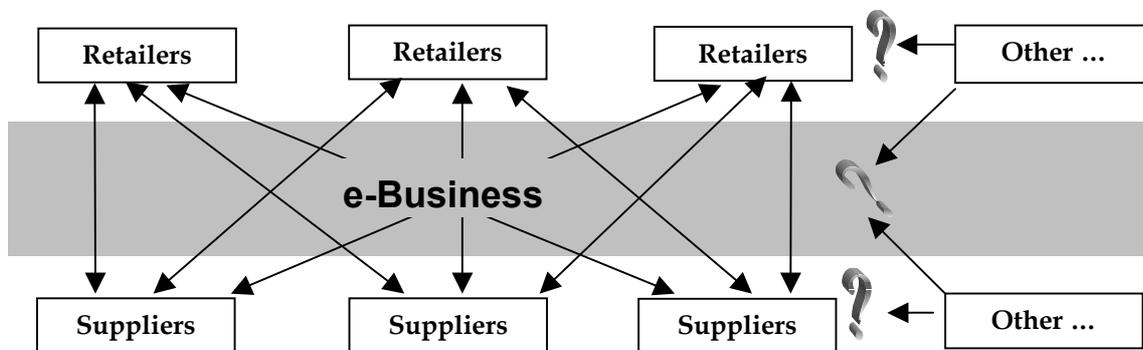


Figure 2 - Model of the Electronic Market

(Adapted from Baron, Shaw, and Bailey, [1, p.94] & Weill and Vitale, [10, p.186])

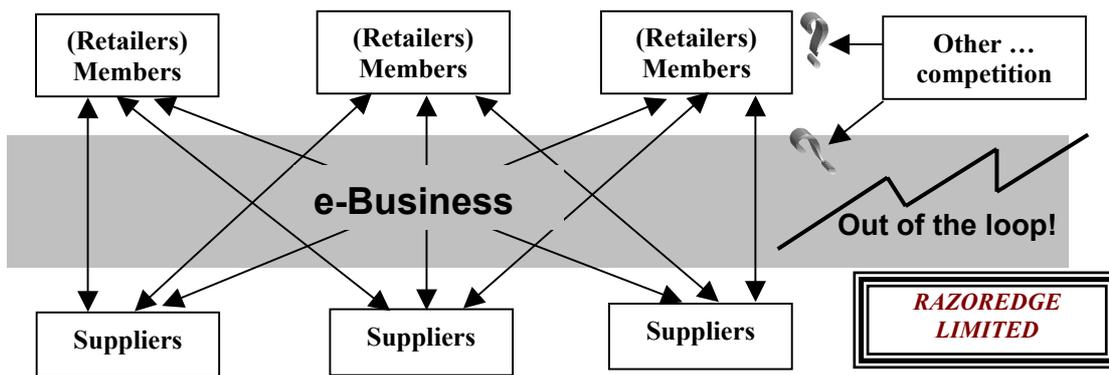


Figure 3 - The threat of the Electronic Market

The above model (Figure 1) represents *RazorEdge Limited's* current operations. It illustrates the major relationships that the company has maintained to achieve its business goals.

In evaluating the risk faced by *RazorEdge Limited*, the model of the electronic market (Figure 2) is an important consideration. This model has information technology

serving as a key component in creating the market. Individual firms operate within the electronic market using technology as an intermediary to interact with end customers. It allows firms to compete in an open market, while allowing customers to select from a variety of potential suppliers.

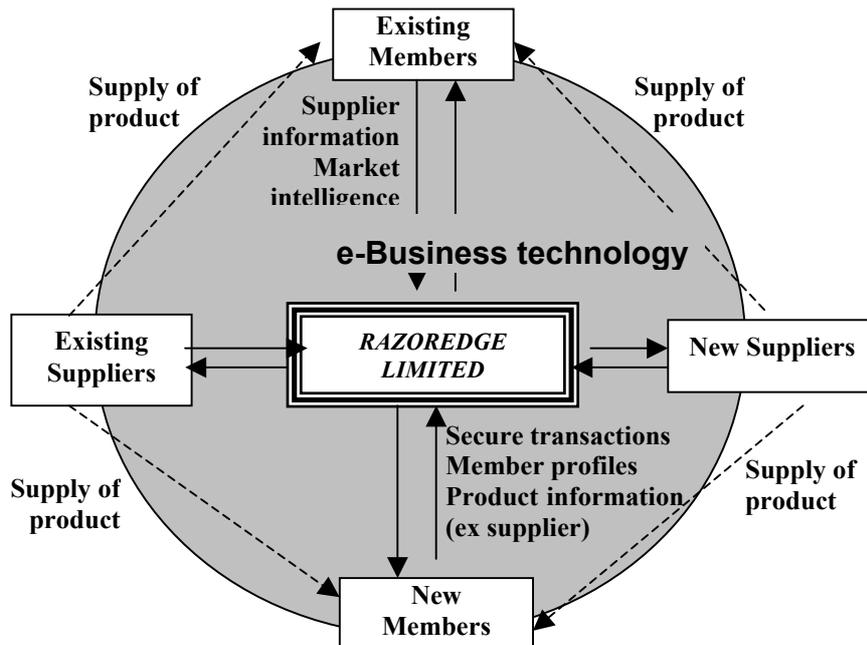


Figure 4 - Suggested model for *RazorEdge Limited*

As can be seen in the model in Figure 3, the Electronic Market is a potential threat to the continued operations of *RazorEdge Limited*. Therefore Figure 4 is a suggested model for *RazorEdge Limited* to minimise risk while achieving the key objectives.

In planning an implementation strategy based upon this model, *RazorEdge Limited* took into account that the e-business environment is characterised by rapid change in two critical areas:

- Information technology, the Web, and associated applications are constantly being developed and improved.
- The “users” understanding of their needs and the potential of e-business is also subject to growth. This can lead to considerable change in the system requirements.

Therefore traditional system implementation approaches are not ideal in this situation. Rather, it is recommended that prioritised initiatives be undertaken in a series of “short time-boxes” – one month duration – development cycles. This is an approach that has been developed for object-oriented systems development, which is closely aligned with e-business [4, pp.21-22]. These short development cycles, and the opportunity for frequent replanning are the critical elements for success. The suggested process is as follows:

- Identify the initiatives to be undertaken, and using these set priorities. The initiatives with the highest priority will be the first to be undertaken. Generally speaking, this will include review of the extendibility of the system architecture, as this will provide a component of the framework for future development.
- Plan the “project activities” for the next two months. Need to consider:

- Which knowledge elements to start with?
- What to develop first?
- What platforms to use?
- What roles and policy to establish?
- Regularly – 3 monthly or sooner if needed – review the initiatives and reset the priorities as required by the “current reality”.

Applying this to the *RazorEdge Limited* case, the following prioritised initiatives were established:

1. Product information - must be accurate, relevant and up-to-date.
2. Company information - including member profiles and supplier details.
3. Push information – trial intelligent agents to push product to market.
4. Develop membership community - with the focus on *RazorEdge Limited*.
5. Develop communication and negotiation support.
6. Information management - details of member history, delivery of orders, and claims.
7. Transactions capture – collecting details of transactions at line-item level.

The first three initiatives were successfully undertaken and implemented. The project was then reviewed and subsequent priorities replanned to accommodate the changing business conditions.

5. Conclusion

Before committing an organisation to an e-business project the following risk-oriented questions should be examined.

1. What is the combination (if any) of e-business models? This should also consider the sources of revenue, and whether they are realistic.
2. What customer segments are targeted, and what is the value proposition to each customer segments?
3. Who owns the relationship, data, and transactions, and what is the likely intimacy of the customer relationship? There is also a need to identify what are the channels to the customers and are they capable of supporting the required richness of information provision and capture?
4. What are the critical success factors, core competencies, IT infrastructure capability and the key information necessary to succeed?
5. What conflicts are inherent in the e-business initiatives?

References

- [1] Baron, J.P., Shaw, M.J. & Bailey, A.D. Jr. "Web-based E-catalog Systems in B2B Procurement," *Communications of the ACM*. 2000, 43 (5), 93-100.
- [2] Becker, T. "Rating the impact of new technologies on democracy," *Communications of the ACM*. 2001, 44 (1), 39-43.
- [3] Greenstein, M. & Feinman, T.M. *Electronic Commerce: Security, Risk Management and Control*. Irwin McGraw Hill, 2000.
- [4] Larman, C. *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design*. Prentice Hall PTR, 1998.
- [5] Lewis, T. "Innovation equals risk reduction," *Computer*. 2000, 23 (10), 112.
- [6] Netscape, *SSL 3.0 Specification*. 2002, <http://www.netscape.com/eng/ssl3/> (Accessed on 15 May 2002).
- [7] Schneider, G.P. & Perry, J.T. *Electronic Commerce*. (2nd ed.) Course Technology - Thomson Learning, 2001.
- [8] Schwalbe, K. (2002) *Information Technology Project Management*. (2nd ed.) Course Technology - Thomson Learning, 2002.
- [9] SET Secure Transactions LLC, *SET Secure Transactions LLC Home*. 2002, <http://www.setco.org/> (Accessed on 15 May 2002).
- [10] Weill, P. & Vitale, M.R. *Place to Space: Migrating to eBusiness Models*. Harvard Business School Press, 2001.