IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

#ITP4361

Method over Mayhem in Managing e-Commerce Risk

Dieter Fink
Associate Professor, School of MIS, Edith Cowan University, Pearson Street, Churchlands WA 6018, Australia
Telephone 61-8-9273872; Fax 61-8-9273; Email d.fink@cowan.edu.au

ABSTRACT

Under the system of e-commerce, organisations leave themselves open to attack which can have catastrophic consequences. Recent well-publicised business disruptions to firms such as Northwest Airlines and Ebay have had significant business impacts. The paper identifies the differences in risk management approaches for older Information Technology systems and those required for e-commerce. The benefits and the critical success factors for an e-commerce risk management methodology are identified and discussed. A literature survey revealed the existence of only two methodologies with potential suitability for e-commerce risk management. They are evaluated against the critical success factors. The paper recommends a program of research to make risk management more dynamic and interactive particularly for the operational aspects of e-commerce.

INTRODUCTION

E-commerce is a multi-faceted business where organisations sell their products to consumers, business combine with other businesses to form virtual enterprises, and suppliers link with partners in a virtual supply chain. The driving force behind the new digital economy is the Internet and technologies, such as the World Wide Web (Web), underpinning this network of networks. The Internet can be described as a non-hierarchical, democratically structured, collaborative arrangement entered into by millions of network users.

Organisations practising e-commerce leave themselves open to attack and compromise which can have catastrophic consequences. New forms of crime are developing (e.g. denial of service) which have not been experienced before. These inherent insecurities require that stringent Risk Management (RM) practices are adopted. However, because of the speed with which network topologies, services and applications change and the whole interconnected nature of the business world in an e-commerce environment, RM systems must operate in a dynamic way. E-commerce is starting to create a true 'just-in-time' economy and RM approaches need to reflect this.

In this paper we recognise the potential for mayhem in e-commerce if risk is not adequately managed. We then proceed to identify the risk areas of e-commerce and compare these with the traditional forms of IT risk. To cope with the new risk environment we outline the benefits of using RM methodologies and survey the literature to establish the existence of e-commerce oriented RM methodologies and their suitability according to criteria we established from our analysis of e-commerce risks.

POTENTIAL FOR MAYHEM

Computer systems employed to facilitate e-commerce "will become the new form of catastrophic exposure that will replace earthquakes and hurricanes as the number one form of catastrophic risk" according to Mullaney of F&D/Zurich (quoted by Hays, 2000). Gow of ACE USA holds a similar view; "If a major operation's network is intentionally compromised, it could interrupt a daily revenue in the millions" (quoted by Hays, 2000) The major compromises for e-commerce were identified as hacker's blackmail, corruption of data, disgruntled employees and unauthorised acts of system administrators.

There are changes taking place within e-commerce that have the potential for significant damage. The consequences of someone meddling with the Web site can range from mild (e.g. the introduction of a detectable virus) to catastrophic (a prolonged system outage leading to the loss of customers). Then there are risk such as out-of-date information, misinformation and defamation on the Web site, even if only there for a brief period, that can lead to lawsuits and claims for damages against the organisation. Added to this is the uncertainty of jurisdiction since the physical space has been replaced by the virtual space. "The velocity and scope of disasters that occur in cyberspace have no real boundaries" (Davis, 1999). The Internet is being called a 'legal vacuum'.

Negative consequences of using the Internet have been experienced by organisatons and have been well publicised. Disruptions in e-commerce have led to lawsuits, significant losses and dissatisfied customers. Table 1 shows recent e-business outages and the business impact they had.

Table 1 E-Business Outages and their Impacts

Company	Industry	Disruption	Business Impact
TD Waterhouse	Financial Services	Extended telecommunications and e-business outage	Significant financial losses
Ameritrade	Financial Services	Multiple system outage due to technical architecture weaknesses	Law suits from online traders. Significant financial losses
Northwest Airlines	Transportation	Multiple system outage	Decline in customer satisfaction
Ebay	Online Auction	Multiple system outage due to technical architecture weaknesses	Significant financial losses
Etrade	Financial Services	Multiple system outage due to technical architecture weaknesses	Law suits from online traders. Significant financial losses
CIHost	Internet Hosting	Extended system outage	Class action lawsuit from online customers. Significant financial losses. Decline in market position/ perception.

(Source: Project Management Institute - Risk Management Specific Interest Group, 2000)

CONTRASTING ITS WITH E-COMMERCE RISKS

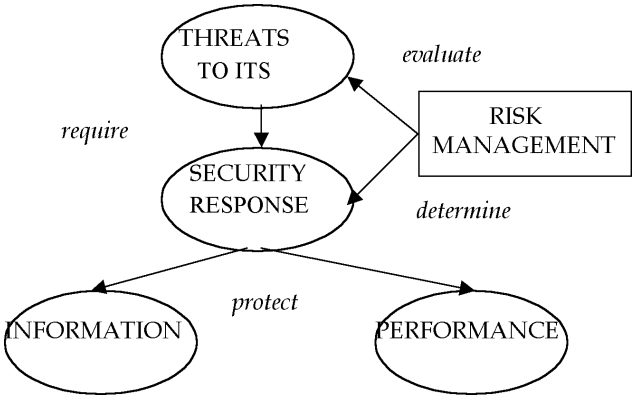
The most common form of RM takes the approach of *risk reduction*. Under this approach, the likelihood or the impact of a threat is reduced to the level considered acceptable for the costs of implementing the security measure that reduces the threat. With *risk avoidance*, the organisation does not accept a threat and does everything within its power to prevent it from occurring. An example is the installation of an emergency power generator to eliminate the risk of being without power should the normal power source fail. Under *risk transfer*, the responsibility for the risks and costs

This paper appears in the book, *Managing Information Technology in a Global Economy*, the proceedings of the Inforrmation Resour es Management Association International Conference. Edited by Mehdi Khosrow-Pour.

are passed to another party, such as an insurance firm.

Risk reduction in RM is practised in many industries (e.g. in banking during loan approval) including by organsations to protect their Information Technology and Systems (ITS). They use RM to determine threats, ITS to be protected and security measures needed to act against threats. In the case of ITS, the major assets to be protected consist of the organisation's valuable information resource and the continuity of its business operations. The dependencies between threats, security response, and resources to be protected in the form of information and performance, are shown in Figure 1.

Figure 1 The Traditional Processes of ITS Risk Management



(Adapted from Fink, 1997)

With the introduction of e-commerce, the ITS environment has changed substantially and business is no longer conducted 'as usual'. While some of the risks associated with e-commerce are not new (e.g. hacking, theft of intellectual property), new implications have arisen because of the far-reaching scope of e-commerce. Old risks have been given a new twist in an e-commerce environment. To understand the new risk environment it is necessary to contrast it with that of the previous ITS environment.

Closed vs open systems

With previous generations of IT, systems were less accessible and open to attack. For example, damages to stand alone systems and local area networks (LANs) are restricted inhouse. E-commerce systems, on the other hand, provide increasing levels of connectivity and accessibility to data and networks from outside the organisation. Losses dues to prolonged system outage are potentially much larger since they are noticed by the outside world and will lead to loss of business and custom.

Tangible vs virtual assets

Traditional ITS environments are more tangible and were easily recognised as data processing centres. With e-commerce, information and virtual trading communities are more difficult to track. Intangible assets are important and take the form of intellectual property, information and knowledge, trademark, patents, copyright. Risks associated with virtual assets (e.g. breach of copyright) are difficult to manage and the courts have been vague about matters of online liability. The absence of physical locations complicates the RM situation.

Development vs operations

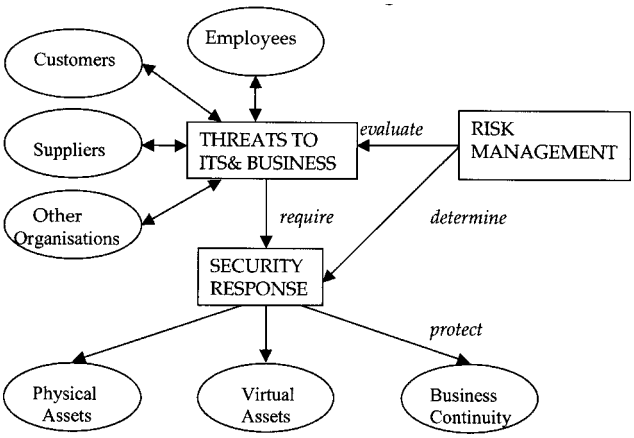
Systems in the past were developed in a controlled manner and released for operations after extensive testing. They were maintained during their life to add new functions and to rectify any problems. With e-commerce, the need for market responsiveness requires that system are developed and operated in a very short time. Operations have become critical because e-commerce aims at high transaction rates in order to bring down the costs of transaction processing. Greater emphasis is therefore placed on operational risk management (McEachen, 2000). Any prolonged system outage will have severe consequences.

Predictability vs volatility

In the past, risk and security management could take place at a leisurely pace and reviews were conducted every couple of years. The RM culture for traditional ITS is unlikely to be satisfactory for the e-commerce environment. It was developed in the early days of computers when IT security could be ensured through physical measures or through the use of closed networks. With each development of an e-commerce function, new elements of risk emerge and uncertainty arises. Examples of current issues and our lack of ability to deal with them efficiently include contractual issues, legislation, taxation, liability, financial exposure and reporting (see McDonald, 2000) to mention a few.

Compared to the RM processes of older ITS (see Figure 1), those for e-commerce have become more complex and greater inter-dependencies have to be considered. Furthermore, the nature of assets to be protected has changed and business continuity has become critical. The changes are reflected in Figure 2.

Figure 2 The Processes of e-Commerce Risk Management



RM METHODOLOGIES AND BENEFITS

With the increased complexity of e-commerce, compared to former generations of ITS, the need for a methodological approach to RM has increased. A methodology can be described as a "A logical and systematic method of identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that enables organisations to minimise losses and maximise opportunities." (Standards Australia, 1999) For e-commerce it is essential that RM methodologies build on the generic fundamentals of RM but develop approaches that meet requirements of the new networked, virtual environment. These specialised requirements are identified and outlined in the following section of the paper.

The generic approach to RM is reflected in standards that have been developed for security management over time. In the UK, BS7799 provides a code of practice for information security management. A key component of these standards is the require-

ment that risk assessment is carried out. The standard allows compliant companies to publicly demonstrate that they can safeguard the confidentiality, integrity and availability of their customers' information. Standards have the potential to become the de facto 'seal of approval' in the world of e-commerce.

Similar standards exist in other countries. In Australia, AS/NZS4444 is based on BS7799 and establishes a code of practice for selecting information security controls (AS/NZS4444.1) and specifying an information security management system (AS/NZS4444.2). As does BS7799, both parts of AS/NZ4444 require that a risk assessment process is used as the basis for selecting controls (treating risks). If an organisation wants to trade securely over the Internet it should ensure that both itself and its partners have this accreditation.

While it may appear that there are overheads associated with the adoption of a RM methodology, there are a number of significant benefits associated with its use.

Stakeholders participation

Information security is often seen solely as the domain of IT professionals with information security being viewed from a technological aspects, i.e. implementing technological measures such as firewalls and encryption. Kelly (1999) refers to this practice as "point solutions" – quick fixes that can do more harm than good. Management and users appear rarely involved in the process. With the increasing integration of ITS in all business activities, as occurs with e-commerce, stakeholders from all areas of the organisation need to be involved. A methodology can provide the framework that will ensure representatives from all business operations participate in risk management.

Holistic

"Many security problems are caused by all too human misperceptions of where dangers actually lie and the ability of particular measures to avoid them." (Brewer, 1999) The levels of security understanding of security threats, exposures, safeguards, practices and priorities among information users and solution providers varies widely. Risk management therefore needs to be approached in a systematic manner so that all perceptions are included and evaluated. A RM methodology provides an approach in which all perceptions, covering all aspects of e-commerce, are captured, analysed and communicated.

Competitive advantage

RM and security activities are seen as burdensome practices that create additional work for already stretched resources. They are often perceived to be only needed when the organisation is under attack or special circumstances arise. This negative perception needs to be reversed and instead a perception that RM can become a competitive advantage to the firm needs to be created. Security should be seen as an enabler since, by operating safely, the organisation can take more risks than its competitors. RM has the obvious advantage of preventing expensive system outages.

CSFS FOR E-COMMERCE RM METHODOLOGIES

RM for e-commerce is different to RM for older ITS because of the differences in their risk profiles (see earlier discussion). An e-commerce RM methodology should nevertheless build on the fundamentals of good security management principles. These can be summarised as follows. "Generally, information security risk management methods and techniques are applied to complete information systems and facilities, but can also be applied to individual system components or services where this is practicable, realistic and helpful. It is an iterative process consisting of steps, which, when undertake in sequence enable continual improvement in decision making." (Standards Australia, 1999) Based on these principles, and the need to consider technology and business risks, a number of Critical Success Factors (CSFs) for an e-commerce methodology can be identified as follows.

Is the methodology effective for e-commerce?

Comprehensive

It must cover technical and business scenarios that are part of the various types of e-commerce (business-to-business, business-to-consumer), the phases of the e-commerce development (from planning to implementation) and the life cycle of operations (from ordering to supply and payments).

Inclusive

The methodology must cover all assets, vulnerabilities and threats. They include technology and business assets, real and virtual, by themselves as well as their interactions. With e-commerce, technology and business are integrated and work synergistically together to achieve maximum impact.

Flexible

It must offer a variety of techniques that can be applied across some or all phases of the methodology. Traditionally, an organisation's assets and policies may have been static but threats in e-commerce are mobile and mutable. Threat levels can rise and fall during a single day's operations as new sites come online or a new virus emerges.

Pro-active

The methodology must be flexible and promote pro-activity to anticipate changes in the e-commerce environment. It should encourage pro-active behaviour that uses RM to gain competitive advantages. To be effective, the methodology should provide a simple approach suitable for an inherently dynamic environment..

Relevant

RM should lead to the identification and application of security measures relevant to e-commerce. Security techniques for e-commerce include the installation of firewalls to separate the 'untrusted' outside networks from trusted internal ones, the use of digital signatures and certificates, encryption, etc.

Will the methodology provide a competitive advantage?

Credibility

The RM methodology should comply with an accepted standard such as BS7799, and should be supported by a credible vendor who is able to provide training, support, documentation, updates, consulting and implementation services. Furthermore, it should offer accreditation by reputable associations and industry bodies.

Value

The cost of the use of the methodology should be covered by the benefits realised from its use. In the real world, resources are limited and decisions about trade-offs have to be constantly made. The RM methodology should be easy to justify in terms of the advantages it provides.

Integration

With e-commerce it is imperative that decisions are made based on both business and technological considerations. Risks in

the technological domain interact with those in the business domain and a RM methodology should cover both types of risk.

Can the methodology be implemented readily?

Systematic

The processes of RM should be structured and systematic to encourage organic management behaviour, transparency and open communications. Guidelines should be available for processes to be followed and the deliverables to be produced for each activity and phase.

Adaptable

The RM methodology must be able to be customised to the existing ITS environment, organisational culture and resource constraints with the objective of making an uncertain environment more certain.

Timely

The methodology must be carried out speedily because of the rapid changes that can occur for e-commerce. It must therefore define procedures, deliverables and timelines that can be applied to small as well as major changes. A speedy implementation of the methodology is essential so that the fluency and flexibility of e-commerce is ensured.

Tracking

With increased operational risk emerged the need to measure and monitor risk factors through risk indicators and metrics. A risk management methodology should provide the system for this and ideally produce dollar-at-risk-type figures.

Sponsorship

It is generally accepted that projects fail if not supported by senior management. They should therefore be an integral part of risk and security solutions. The e-commerce sponsor should have an active involvement in implementing the RM methodology and be satisfied with risk outcomes before releasing further funding for the e-commerce project.

SURVEY OF E-COMMERCE RM METHODOLOGIES

A search of the Web and our university's online library database revealed many papers discussing the nature of e-commerce risk but very few that addressed the requirements and practices of RM for these risks. The literature on e-commerce risk appeared to be dominated by opinions held by the insurance and finance industries. These industries have long used RM to assess the risk of their clients and are developing an interest in providing insurance coverage to organisations with e-commerce activities.

In the absence of suitable methodologies on how to manage the risks associated with e-commerce, it is not surprising that the increased levels of concern have given rise to reactive approaches in the form of protective insurance (Hays, 2000). Companies with a high volume of e-commerce are under pressure from shareholders to ensure that their operations stay afloat and, according to Mullaney of F&D/Zurich, will have to "buy a risk transfer product or install a solution" (quoted by Hays, 2000).

At present, however, insurance does not provide a complete solution to organisations concerned with e-commerce risk. First, "Traditional insurance companies insure property losses and liabilities but not those that arise from e-commerce" (Davis, 1999). Second, "Currently there are fewer than 10 agencies that offer e-business insurance" (Davis, 1999). Organisations therefore have to look to other solutions particularly RM methodologies to manage e-commerce risk. Our literature search, however, revealed only two methodologies that were associated with the use of e-commerce. They are outlined below.

Active Risk Management (ARM)

The ARM approach appears to be supported by the Project Management Institute Risk Management Specific Group since it was outlined in its March 2000 newsletter (www.risksig.com/signews/Rmnews0003.pdf) whose theme was 'Continuity in a Virtual World'. In the newsletter, Parker (2000) outlines the ARM methodology which he describes as "a discipline and environment of proactive decisions and action to assess continuously what can go wrong, determine what risks are important, their impact, and implement a strategy to deal with those risks."

ARM's primary aim is to manage risk in a software project, and its proactive philosophy and methodical approach makes it potentially useful to e-commerce systems. Parker (2000) emphasises that ARM is an ongoing process and not a static project task. It includes three major phases- risk identification, risk analysis, and risk control. Phase 1 (risk identification) is accompanied by a questionnaire that narrows the focus on particular aspects of risks and assists in identifying risks during a project in the areas of requirements determination, design, code and unit test, integration and test, and communications and team motivation.

In Phase 2 (risk analysis), risk probability, risk impact, risk exposure and risk consequences are 'quantified' as best as possible. Where quantification is not possible, qualitative categorisation is applied. For example, an impact/probability matrix determines risk exposure as very high, high, medium, low and very low. Phase 3 (risk control) defines steps to avoid, mitigate or accept for risks identified in the previous phase.

CCTA RISK ANALYSIS AND MANAGEMENT METHODOLOGY (CRAMM)

CRAMM is a formalised, structured security risk analysis and management methodology developed by the British government. It is regarded by many as the de-facto standard for risk analysis and management. It has been described as "an essential first step towards BS7799, the standard for information security management" (Logica) and is consistent with the European IT Security Evaluation Criteria (CRAMM User Group). Even though CRAMM was developed in the early days of computers, it has undergone changes with newer versions reflecting the requirements of new ITS environments. Version 3.0, released in 1997, is implemented as an interactive software tool for identifying the security requirements (Gamma).

A CRAMM review may be undertaken during systems development or retrospectively for completed systems and proceeds through three stages: identification and valuation of assets, quantification of likely threats and known vulnerabilities, and generation of countermeasures. CRAMM includes a countermeasures database which provides three levels of detail: security objectives, detailed countermeasures descriptions and implementation examples.

At the completion of each stage, formats can be extracted which can be in redefined and customised. CRAMM enables the building a model encapsulating asset interdependence and information on which parts of the system support which business processes. This provides insight into operational characteristics which is critical in an e-commerce environment.

Based on the information we were able to gather, we attempted to evaluate the two methodologies against criteria for a

suitable e-commerce RM methodology we had established (see earlier section). Table 2 reflects our assessment.

Table 2 Evaluation of e-Commerce RM methodologies

CSFs	ARM	CRAMM
Effectiveness		
Comprehensive	√	√
Inclusive	√	√
Flexible	√	√
Pro-active	√	√
Relevant	?	√
Competitive advantage		
Credibility	√	√
Value	?	?
Integration	√	√
Implementation		
Systematic	√	√
Adaptable	√	√
Timely	√	√
Tracking	?	?
Sponsorship	√	√

CONCLUSIONS AND FUTURE RESEARCH

Our preliminary findings indicated that both methodologies have strong potential to provide the necessary guidelines to assist an organisation reduce the risks of e-commerce. CRAMM appears to have an advantage over ARM because it offers a countermeasure database. We are not familiar with the security and control measures included in this database but assume that they would have relevance to e-commerce because the latest version of CRAMM had been released fairly recently. As seen in Table 2, we were not able to draw a conclusion as to the tracking capabilities of the methodologies or their values because of the lack of detailed information.

Our research is of an exploratory nature and established the scarcity of RM methodologies designed for e-commerce. As e-commerce becomes mainstream, the demand for such products will increase. Our paper identified the benefits and the essential criteria for evaluating RM products that may emerge in response to this expected demand. This should provide useful insight and information to managers responsible for e-commerce risk and security.

There are a number of opportunities for researchers to support the development of e-commerce RM methodologies. As identified earlier in the paper, e-commerce requires emphasis to be placed on operational risk management. To manage operational risk requires definition and identification of key factors, such a data collection and communicatons, and key risk indicators and risk measurement metrics. A risk management methodology should provide the system for this and ideally produce a dollar-at-risk-type figure. However as Deborah Williams of Meridien Research (quoted in McEachern, 2000) points out, few vendor packages in the RM domain currently provide such output.

In future, the speed with which new networking and operating architectures and applications will emerge could outstrip the ability of management to keep up. If they can't, it will severely limit the organisation's ability to exploit new business possibilities. New generations of methodologies that automate the process of RM will be demanded. Researchers should assist in the development of RM methodologies that are able to scan a network and produce real-time analyses of vulnerabilities and effective countermeasures in forms that senior executives can understand.

REFERENCES

Brewer D (1999) "Keeping Virtual Worlds open for Business", *Telecommunications*, 33(9), 65-66.

CRAMM User Group "What is CRAMM?" (online) www.crammusergroup.org.uk

Davies R. (1999) "Taking the Risk out of e-Commerce", *Techwatch*, October, 45-46.

Fink D. (1997) *Information Technology Security - Managing Challenges and Creating Opportunities*, CCH Australia, Sydney.

Gamma "CRAMM" (online) www.gammassl.co.uk/topics/hot5.html

Hays D (2000) "Insurers Cover Hackers' Threat to E-commerce", *National Underwriter* 20-25.

Kelly B.J. (1999) Preserve, Protect, and Defend, *The Journal of Business Strategy*, 20(5), 22-25.

Logica "CRAMM, IT Security Risk Assessment and Management" (online)
www.logica.com/offerings/CRAMM.html

McEachern C. (2000) "Infinity launches e-Commerce Strategy, Internet Risk Applications", *Wall Street & Technology*, May, 62.

Parker G. (2000) "Active Risk Management" (online) www.risksig.com/signews/RMnews0003.pdf

Project Management Institute – Risk Management Specific Interest Group "Risk Management Newsletter", (online) www.risksig.com/signews/RMnews0003.pdf

Standards Australia (1999) (online) www.standards.com.au/Catalogue/Script/Details.asp?DocN=stds000023835