RISK MANAGEMENT IN THE DIGITAL AGE

MANAGEMENTUL RISCULUI ÎN ERA DIGITALĂ

LUMINIŢA ŞERBĂNESCU[1]

[1]University of Pitesti, Romania; luminitaserb@yahoo.com

Abstract: *In recent years dynamic internet-based start-ups have captured the public imagination through the creation of revolutionary business models. As we are now seeing, many lack the financial stamina to survive and become profitable. Attention has switched to how established companies are trying to clone these new models to their competitive advantage. However, in the rush to do so, many organizations are making quite fundamental strategic mistakes; mistakes that are often then repeated by others. This may be because they have failed to recognize the need to apply advanced risk management thinking to both the strategic and implementation issues surrounding the E-business imperative.*

Keywords: *e-business, strategies, technologies, security*

INTRODUCTION

The essential characteristic of information societies is the integrated, massive and generalized usage of the means of processing information and communication in all the fields of socio-economic life, from commodity production to services, administration and ending with artistic activities and citizen services.

The Internet plays a key part in providing information regarding the availability of services and products as well as their price in the whole economy. The new Internet technologies contribute directly to the expansion e-commerce and the new business and e-business models.

Information security technologies, especially when the information is distributed in computer networks, are absolutely necessary in order to ensure success, and as a result, they must be included in the process of strategic thinking of a company. Information security must be seen as an essential process in satisfying the partner and clients' legitimate needs and not as something "additional". On the other hand, the companies have to make sure that their marketing and public relation departments are

conversant with the principles of information security technologies so as to inform the public on the measures which are taken in order to protect the clients' money and privacy.

MATERIALS AND METHODS

It must be specified that the new economy, also named digital economy, is based on three defining principles: access/ instantaneous response; personalized services; simultaneous presence in different locations.

The modern business environment is characterized by an unprecedented increase in the providers offer, in the global competition and in the clients' exigency. Companies from all business segments have begun to embrace the new economic paradigm – e-business or new business models.

E-business can be defined as the transformation of the constitutive processes of a business (operations, components) with the aid of web and internet technologies which allows business to be active 24 hours a day.

Choosing the business model is the first decision to be made when an on-line business is started. The new business model involves a chain of electronic services, consisting of:

- the provider of the required services and products;
- the provider of Internet services who can offer everything, from web space to e-mall integration and different types of services;
- the client, with a certain profession, personal interests and preferences. The client can be a consumer (B2C), another business (B2B), public administration (B2A) or an employee (B2E).

Electronic commerce will lead through its development to: the increase of labor productivity; the intensification of the flow of goods and services; investments development; the creation of new sectors; diversification of marketing and sales forms. It will generate an impact on a large number of economic activities that will be reconsidered and restructured in order to cope with the new requirements.

The fundamental principles of an electronic business are the same as those of any traditional business, carried on in a real economic environment: there is a target public and a product or service offered for sale. As a result of the meeting between the demand and offer, the consumer will receive the

product, and the producer will collect its counter value, i.e. the producer will invoice the counter value of the service provided for the consumer, and will collect the appropriate sum of money.

The major difference between the two forms of business is that electronic business allows the automation of selling and buying processes. In an ordinary shop there are employees that help the customer to buy. In the case of virtual shops, the employee is replaced by the site itself that works 24 hours a day, seven days a week, during a whole year without break in order to maximize the business profit.

There are four main impediments that slow down the development of e-commerce:

- *security*: the Internet was conceived as an open environment, but not necessarily a secure one, the Internet Protocol Suite (TCP/IP) lacking basic security services. An elementary constituent that ensures security of commerce on the Internet is the crypt which guarantees both the authentication and the security of sending information;
- *acceptance of new forms of payment (electronic money/ digital cash)*: the main problem is the private way in which money is normally spent. It is the problem of supervising transactions. An electronic system that records all the transactions that are made on the cyberspace has the disadvantage that everything one does is recorded;
- *the costs of investments*: for example a tradesman who wants to offer a shop on the Internet, will make the following investments: servers, communications technology, e-commerce software, technologies that ensure security, for example the firewalls;
- *the legal and normative framework*: refers to all the aspects of the fiscal framework, intellectual property rights, consumer data protection.

DATA SECURITY STRATEGIES IN E-BUSINESS

Data security in economic information systems can be defined as a set of measures taken by the economic agent in order to ensure the information secrecy against unauthorized access.

Security technologies for economic data have many components and attributes that should be taken into account when the potential risk is calculated. Generally speaking, they can be divided into four main categories::

Privacy refers to data protection in the system which prevents it from being accessed by unauthorized persons. We are talking about the control over the right to read information. Almost any organization has information which, if divulged or stolen, may have a significant impact on the competitive advantage, the market value or earnings. To ensure privacy it is important to know which information is to be protected and who must or must not have access to it. This implies the existence of protection mechanisms stored in computers that are transferred in a network between computers. On the Internet, privacy gains new dimensions in the form of privacy control measures.

Integrity represents data protection against unauthorized intentional or accidental changes. It refers to the need to make sure that the information and programs are modified only in the specified and authorized manner and that the data is original, unaltered or deleted in transit. As in the case of privacy, user identification and authentication is a key element of an information integrity policy. Integrity is particularly important for critical safety and financial data used in activities as electronic funds transfers, air traffic control and financial accounting.

Availability refers to making sure that calculation systems are accessible to authorized users whenever and wherever they need it in the needed form. The importance each of these requirements plays in the operations performed by a company differs from industry to industry and from company to company. Availability is often the most important attribute in service oriented business which depends on information (air scheduling and online inventory systems). Network availability is important for any person whose business or education depends on network connection. When a user cannot access the network or a specific service provided on the network, he experiences a refusal of that service.

The purpose of information security technologies consists of protecting the interests of those who rely on information and the means of communications which deliver the information against the losses which result from the incapacity to ensure the availability, privacy and integrity of information.

Non-repudiation is characteristic of the transactions in which the parties in a conducted transaction are certified, so that none of the parties involved can deny its participation or the details of the actions or decisions made during the participation. Non-repudiation is the basis of digital

signatures, ensuring their authenticity on the new market of electronic commerce.

DATA SECURITY TECHNOLOGIES

Restriction technologies are meant to limit the access to information. Part of this category is:

1. *Access control* is a term used to define a set of security technologies that are projected to restrict access. This means that only the persons who are given permission can use the computer and have access to the stored data. The term of access control defines a set of control mechanisms implemented in the operating systems by producers in order to restrict access. Operating systems such as Windows, UNIX, and Linux benefit from this facility.

2. *Identification and authentication*, using accounts and passwords, allow access to the information only to the authorized users. Identification and authentication can be made with the aid of electronic cards (smart card) or of biometric methods (fingerprint, voice, eye iris etc).

3. *The firewall* is a software filter that stops certain preset traffic from the networks and allows its passage. At the same time, the firewall can be used in the own network to separate different sub networks with different levels of security.

4. *Public key infrastructure (PKI)* aims to ensure security in open systems, as the Internet, and to assure the trust between two persons who have never met. In a PKI complete structure, each user will be completely identified through a guaranteed method, and each message he sends or application he launches is transparent and completely associated with the author.

5. *Single sign-on (SSO)* aims to help the user get rid of the multitude of accounts and passwords that have to be introduced each time s/he accesses or re-accesses programs. The user has to authenticate only once. The aspiration is difficult to accomplish because of the variety of systems. For the moment it can be used by companies that have the same type of systems. The web uses a SSO subset named Webs SSO, which can be used as web servers use the same technology.

Besides the restriction technologies system security must be administrated, monitored and maintained. This implies: administration, intruder detection, vulnerability scanning, and virus control.

RESULTS AND DISCUTIONS

Almost all people and organizations strive to manage risk for three fundamental reasons:

- To safeguard resources from surprising losses. Safeguarding the resources which a person or organization already possesses involves either reducing the surprising losses to which these resources are exposed or restoring them from losses that they experience. These two basic strategies for safeguarding resources rely on either risk control or risk financing techniques.
- To be prepared to seize surprising opportunities. Remember that risk can bring surprisingly favorable outcomes as well as surprisingly unfavorable ones. People and organizations that safeguard their resources against the surprising losses that often come from unfavorable outcomes are in a better position to seize surprising opportunities than are those who have not protected what they already have.
- To limit uncertainty, both in their minds and in the world. Those who practice effective risk management have a better grip on their future. They know that they have done all they cost effectively can to prevent accidental losses, to reduce the probability and magnitude of any losses they cannot prevent, and to secure funds to finance recovery from any surprising losses they cannot control. They also know that they are ready to act on any unexpected opportunities they may encounter.

Risk management exists precisely because the world is not stable—surprising things, both good and bad, happen. Even the once most nearly perfect risk management program needs to evolve in response to changes in any of the factors that shaped the original program.

These changing factors can be categorized as changes in:

- Loss exposures.
- Organizational goals.
- The cost and benefits of these techniques.
- The attitudes management holds toward risk.

Adapting to the changes in these clusters of factors—changing the program in response to, or in anticipation of, these changing factors—is the last of the four essential steps in risk management. Because change never stops, the process of managing risk never ends.

Risk mitigation measures are usually formulated according to one or more of the following major risk options, which are:

1. Design a new business process with adequate built-in risk control and containment measures from the start.
2. Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.
3. Transfer risks to an external agency (e.g. an insurance company)
4. Avoid risks altogether (e.g. by closing down a particular high-risk business area)

CONCLUSIONS

Regarding the general aspects of ensuring data security in e-business we can conclude that:

1. Ensuring data security is closely connected to the financial conditions of the company. Big and medium companies, with big profit can invest in security. Small companies rarely do that or they do not invest enough to ensure maximum security.
2. In the case of big companies there are specialized personnel to ensure data security. These will implement the security policy of the company and will periodically test the computers in order to detect security holes.
3. In the situations when the company, irrespective of its size, has no specialized personnel in the implementation and administration of security measurements, the company can resort to specialized companies to implement and administrate the security services. They can choose a mixed solution in which the study and the implementation are done by a specialized company and the administration by the beneficiary, and it can be periodically tested by the specialized company.
4. Applicative programs at the level of big and medium companies are elaborated taking into account data security. Small companies use either pirate programs or applications made by unspecialized people that not only do not have security elements but they also work defectively, altering data.

Risk management is simply a practice of systematically selecting cost effective approaches for minimising the effect of threat realization to the organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore all organizations have to accept some level of residual risks.

Whereas risk management tends to be preemptive, business continuity planning (BCP) was invented to deal with the consequences of realised residual risks. The necessity to have BCP in place arises because even very unlikely events will occur if given enough time. Risk management and BCP are often mistakenly seen as rivals or overlapping practices. In fact these processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP (assets, impact assessments, cost estimates etc.). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process.

REFERENCES

1. **COSTACHE, N., VINTILA, C.** (2000) - Managementul sistemelor economice, Transdata Publishing House, Ploiesti.
2. **DEBRA CAMERON** (2000) - Electronic Commerce – The New Business Platform for the Internet, Computer Technology Research Corp.
3. **FOTACHE, D., HURUBEAN, L**. (2004) - Soluții informatice integrate pentru gestiunea afacerilor – ERP, Economic Publishing House, Bucureşti, 2004.
4. **PRESSMAN, R. S.** (2000) - Software Engineering – A Practitioner's Approach, European xAdaptation Fifth Edition, McGraw-Hill.
5. **REBOUT, P., XARDEL, D.** (1997) - Le commmerce Electronique, Technique et Enjeux, Editions Eyrolles, Paris, France.
6. **SUMNER B.** (2006) - Security Management:A New Model to Align Security With Business Needs, CA.
7. **URSĂCESCU, M.** (2003) - Sisteme informatice. O abordare între clasic şi modern, Economic Publishing House, Bucureşti.