raționale, cât și administrative.

- Metoda prețului de piață, a cărei esențe este de a compara valoarea bunului analizat cu valoarea unui bun cu care se operează pe piață în condițiile similare. Dezavantajul metodei constă în faptul că nu întotdeauna există date veridice privind tranzacțiile pe piață.
- Metoda veniturilor, se bazează pe proprietatea creațiilor intelectuale de a genera venit.

Riscurile aferente reproducerii și menținerii securității informaționale.

În această categorie vor fi acelea costuri periodice ce apar în procesul de reproducere sau dezvoltare a bunului. Aceste riscuri sunt invers proporționale nivelului de dezvoltare și integritate a sistemului proprietății intelectuale în țară. De exemplu, costurile pentru litigiile ce sunt mai mari în acelea state, în care protecția proprietății intelectuale nu este o prioritate.

Probabilitatea de succes.

Întrucât caracteristicile principale, care caracterizează piața creațiilor intelectuale sunt flexibilitate înaltă și o viață scurtă a bunului, astfel probabilitatea de succes reprezintă șansa de penetrare a noului bun pe piață.

Problema în analiza acestor bunuri este unicitatea lor, căci majoritatea satisfac anumite nevoi ale consumatorului și înseși bunurile similare diferă în utilitate și potențial.

Bibliografie:

1. Michael Perelman *The Political Economy of Intellectual Property*
2. Середа С.А. *О необходимости защиты прав потребителя в сфере информационных технологий*
3. David Drews *Intellectual property valuation techniques*
4. *www.wipo.org*
5. *www.iipi.org*

Ljupco Davcev,
the Faculty of Economics at the University "Goce Delcev", Stip, Republic of Macedonia

MANAGING SECURITY IN AN E-BUSINESS ENVIRONMENT

Technological developments over the past few years have made significant contributions to securing the Internet for e-business. Ensuring security for e-business information exchange is essential as it entails exchange of sensitive information. E-business transactions entail transfer of funds with buyers, sellers and business partners. Vulnerabilities and security incidents in the digital environment require an understanding of teshnology issues and security challenges

for privacy and trust in an online environment. This paper discuss managing security in a e-business environment. More importantly the paper highlights e-business security management by highlighting the need for organization based security policies, procedures and practices.

INTRODUCTION

The Internet is a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways, including gateways, routers, dial-up connections, and Internet service providers. It is a self-regulated network connecting millions of computer networks around the world (Turban, 2002). Everyone can access the network without regard to national or geographic boundaries or time of day. E-business operates in a networked environment supported by the Internet and other network technologies. Hence, e-businesses are in need of security measures for protection of data transmited, databases, all electronic exchanges of information and other types of cybercrime. A lack of privacy, integrity and confidentiality can cause tremendous damage to an organization and its business, along with its system slowdowns and downtime. It is imperative that e-businesses put in place organizational, architectual and procedural approaches to ensure that the business operates in a secure and reliable environment. E-business security embraces the complete business transaction not only from the IT infrastructure inside an organization's network, but also outside, connecting all customers and suppliers.

E-BUSINESS SECURITY

Ensuring security for e-business information exchange is essential, as it entails exchange of sensitive information. Technological developments over the past few years have made significant contributions to securing the Internet for e-businesses. However, challenges remain in this area, and combined with the business and legal requirements security remains a substantial barrier to e-business development.

In a society, ensuring security involves police and security quards, locks and alarms, but in a commercial environment protecting sensitive data and information, transactions involving financial information, corporate secrets and proprietary information need to be protected. Security for electronic commerce faces several challenges that are inherently not as challenging in paper-based commerce. Some intrinsic characteristics of paper-based signed documents in commerce that quarantee their security, but are absent in electronic commerce are properties of the ink, the letterhead, characteristics of the printing process, watermarks, signature biometrics, timestamps, and ability to setect modifications. However, these attributes are not inherently built into e-commerce technologies.

Potential threats and attacks to which commercial activities in networked environments may be suspectible are accessing unauthorised network resources, destroying information and network resources, altering, inserting or modifying information, disclosing information to unauthorised people, causing networking services

disruptions or interruption, stealing information and network resources, denying services received, claiming to have provided services that have not been administered, and claiming to have sent or received information not given (Adam et al., 1999).

SECURITY POLICY

It is essental that all e-business organizations put in place a security policy at the time of implementation of technologies that will support the on-line business. A security policy is a document high-level plan for organization-wide computer and information security (Minoli&minoli, 1998). It provides a framework for making specific decisions, such as which defence mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues.

Security policy must address the personel in the organization. Physical security of technology, access policy of data and equipment access are initial consideration. Having a physical security policy for IT and e-business equipment is vital for protecting confidential data. Issues included in the physical security policy generally address:

- ensuring the workplace technology supporting e-business is stored in a secure and lockable location
- keeping up-to-date logs of all equipment
- taking out appropriate insurance policies and developing emergency repair plans
- putting extra measures in place for notebook computers(such as encrypting all data stored on them)
- making sure all staff are aware of security policies and report any suspicious activities.

As mentioned earlier, sometimes internal stuff can pose a greater security threat than external hackers, since they allready have access to sensitive information. Polices to minimise internal risks should include:

- making sure passwords and access systems are revoked when staff resign
- not giving any single member of staff complete access to all data
- keeping logs of and documenting access to key business information
- implementing and maintaining a strong password policy
- conducting regular internal security audits.

SECURITY CHALLENGES

Despite advances in security technologies, securing confidential and proprietary information has become more interesting and challenging then ever. In an attempt to keep pace with the onslaught of security woes, new technologies are ofter unleashed and implemented before due diligence and real understanding of these technologies occure in the real world. Though understanding security technologies is noble, and certainly a diligent undertaking, the recent trends in corporate technology deployments have shown that most organizations do not have the resources and time to fully understand the technologies that they are deploying (Larson, 2003).

Security is not black and white. A firewall, if configured properly, will keep out 95%of the trouble makers.But, that 5% is a powerful force that only needs small trinkers of security holes to invade the corporate immune system, and anyone who has worked as part of an incident response team knows that one security has been violated, repairing the damage is time consuming and often creates liabilities with alliance partners, suppliers and customers.

A breach of security can compromise impoortant confidential information about an organization leading to damaging impact on business. The consequences of the break-in in the business network system can be a minor or majot loss of time in recovery for the program, a decrease of productivity, a significant loss of money or stuff hours, a devastating loss of credibility or market opportunity, a business no longer able to compete and legal liability. Data security is vital in the e-commerce environment as critical information is exchanged electronicaly between business partners. E-business operates in a network environment with automated and electronic transmission of data, business informations, payments and negotiation. Also, data transmission and storage thus need to be well secured. Even computers with nothing stored on them should be secured, as thay can become a weak link allowing unauthorized access to the organization's systems amd information.

CONCLUSION

Security management involves the control of liability in digital transactions as well as the establishment and enforcment of security policies to ensure that the requirements for security services be meet in order for a security system to achieve its objectives. Effective management of security will become an essential enabler of e-business. Just as individual consumers tend to avoid business that do not protect their transactions, business partners will certainly avoid companies that don't take adequate measures to protect their databeses and information. Security management needs must receive adequate subsidisation and support from e-business participants for their technology based commercial initiatives to be successful.

References:

1. Adam, N., Oktay, D., Gangopadhya, A., & Yesha, Y. (1999). *Electronic commerce technical, business and legal issues*. New Jersey:Prentice Hall
2. Larson, D. (2003). The race to secure cyberspace. http://www.webdeveloper.com/security/security_race_cyberspace.html
3. Minoli,D.,&Minoli,E.(1998). *Web commerce technology handbook*. New York: McGraw-Hill.
4. Napier,H.,Judd,P.,Rivers,O.,&Wagner,S.(2001). *Creating a winning e-business*. Canada:Thomson Learning.
5. Turban,E.,Lee,J.,King,D.,&Chung,H.M.(2002). *Electronic commerce-A managerial perspective*. New Jersey:Prentice Hall International Inc.