December 2004

The Importance Of eSecurity In The Overall eStrategy Of An Organisation

Aleksander Iinigoj
Palsit

17th Bled eCommerce Conference

eGlobal

Bled, Slovenia, June 21 - 23, 2004

The Importance Of eSecurity In The Overall eStrategy Of An Organisation

Aleksander Šinigoj

Palsit, Slovenia
aleksander@palsit.com

Abstract

Information security strategy is necessary in organizations in order to determine their risks and providing suitable policies and procedures for appropriate controls and countermeasures to manage those risks. Still too often the human factor is underestimated and people do not know how to choose safe passwords, how to react when they find out about a security breach, all that due to the fact that they are not properly trained or educated. Information security is not just a technical issue but also a policy and human issue that requires the use of technology to protect the business information. Our goal should be to clearly define roles and responsibilities of information security officer and all employees in an organization to improve overall security and the protection of that information.

1 The Need For A Clear Strategy

Our society has undergone a profound change. Information systems and information infrastructure in companies have considerably changed in recent years and became more distributed, and as such, much more complex to manage. Business information is dispersed, as local area networks and departmental systems have replaced the centralised mainframes. Only 15% of employees had access to corporate data in 1985, but by year 2000 the number had risen to over 85% (Yapp, 2000, p. 23). Information is an important asset which has a value to an organization and therefore needs to be well protected (ISO/IEC 17799:2000).

The increased dependence of organizations on information and communication technologies and the changed business model due to globalisation and internationalisation has rapidly increased the need for systematic and professional protection of that information. Information security becomes now more complicated and is not restricted only to maintain confidentiality, availability and integrity, but we need to put strong emphasis also on responsibility, integrity and people (Dhillon, p. 1, 2001). Most companies, do not have a written information security policy or e-security strategy, nor they have authorized people that are responsible for information security management.

The human firewall is likely to have more holes in most of Slovenian and worldwide organisation that has the firewall protecting the local area network from the outside Internet.

2 Determine The Risks

Before e-security document in the overall e-strategy of an organisation can be written and be well defined, we need first to determine the overall objective to protect the company and its assets. The first step therefore gives us the answer to the question what is being protected and why is being protected (Barman, 2002, p. 6). We need to learn more about the risks that our company is facing. Risk evaluation and risk management are one of the most important parts of the process for preparing the information security documents (Avolio, 1998). At first we need to classify the value and importance of the assets within the company and then the likely threats and vulnerabilities that are endangering those assets. Too often it is difficult to define the vulnerabilities before an attacker actually is exploiting them.

Therefore many companies decide to outsource different vulnerability assessment services to specialised companies that can check for possible holes and exploits before hackers find them. The proactive approach has proven to be successful and widespread in the financial industries. Nevertheless, in many organizations managing risks is considered to be part of the corporate quality assurance programme due to the fact that protection of important information is seen as a critical business requirement (Broderick, 2001, p. 12). Thus the risk countermeasure implementation and evaluation are used to protect the critical business information from the most important vulnerabilities.

Organisation needs to assess the information security risks taking into account the actual business value of the information and other assets at risk. Can we ensure confidentiality, integrity and availability of the assets, because we highly depend on them. E-strategy that also includes e-security must ensure that we keep the competitive edge, constant or increasing cash flow, profitability, regulatory and legal compliance with the overall goodwill of the organisation. Are we going to suffer losses because of the new computer viruses or worms is our communication encrypted and what is the likelihood of espionage, sabotage, vandalism or other sources of failure or disaster.

3 Social Engineering And The Human Factor

Security has a weak-link dependency, as it is no stronger than its greatest vulnerabilities, if we at least theoretically assume that adversaries have broad capabilities and intent (Parker, 1998, p. 273). The list of vulnerabilities and threats that a company is exposed to can be rather long. System administrators would point out denial of service attacks, viruses, worms, time bombs, web site defacement, corruption etc (Schneier, 2001, p. 493). Vandalism, financial fraud, theft of transaction, data and identity interception, manipulation, misrouting and masquerade remain the most important threats to the infrastructure of an organizations. Internet has also stimulated international commercial espionage where many countries, businesses and secret services have been involved in unauthorised gathering of confidential data.

Organisations are exposed to internal and external attacks. All strategic partners that have access to the information system of an organization we need to ensure that they have

same security standards and controls. Suppliers, customers, partners and employees are often accessing a whole variety of databases (Lothiam and Wenham, 2001, p. 12). Due to this reason Bank of Slovenia has instructed all banks to implement information security policy by using the BS7799 standard (Arhar, 2000). But banks are dealing with all organisations from large to medium and small. Will the let those organisation to access their networks without knowing anything about e-security.

Many national computer systems such as nuclear power stations, defence systems, aircraft flight control could perform high-risk activities. The dangers of hacking into these systems and potential terrorist activities are worrying also after the terrorist attacks on the World Trade Center last year (Bainbridge, 2000, p. 307). The problem remains also in strategic directions of companies, which are spending considerable time, money and effort on implementing different technologies but are not considering of improving security awareness throughout their companies. The importance of improving security culture in companies is still underestimated.

3.1 Building A Human Firewall

Information security needs to consider the human factor in order to be successful. People are often the weakest link for security, yet many organizations are failing to address this (Potter et al, 2002, p. 16). When a company has strong technical controls the criminals try to seek out alternative vulnerabilities and organisations may suffer losses higher than those that controls were designed to prevent (Parker, 1998, p. 6). Social engineering remains one of the most successful methods to break into a system a create certain damage by simply convincing the legitimate users to give us certain information (Kolšek, 2001). Even one of the well known convicted computer criminals Kevin Mitnick confessed that he was so successful in social engineering that he rarely needed to use technical tools. Even good users sometimes do bad things by unwittingly running hostile code on their computers.

There are several threats that our information system can be exposed to due to the human factor: abuse of privileges and trust is quite often and people misuse the systems and network. According to the KMPG survey (2001) system administrators, current employees and lack awareness form some of the greatest threats to our system. They leave their personal computers unprotected, they do not use the clear desk policy and leave many secure documents for potential visitors to see, they install different software games or screensavers without considering that those might be Trojan horses or time bombs.

Lack of employee security awareness is often found also in passwords. Most users gain access to secured sites and databases by entering passwords. People need to remember large number of PINs and passwords, for their electronic mail, different debit and credit cards, phone numbers, some even have passwords to their electronic organizers to have a track of all their passwords. Security policy should clearly define that passwords should be kept confidential and not written on a paper. It should be composed of numeric and alphabetical groups of characters. Users shouldn't use names of their family, pets, addresses or other easily guessable passwords. All those rules reduce the opportunity of unauthorized user access. The responsibility for keeping passwords confidential or regularly updated them, together with logging out from the system or service, should be allocated to each individual user and not to information technology department or even to the head of information security, the information security officer.

Human firewall is the state of the organization where people understand their roles and responsibilities and are trying to improve the security of information and information technology and are empowered to make prudent decisions about security. It is important that also distributors, partners and other external co-workers fully understand our information security policy and are willing to accept it (Samuels, 2002, p. 32). The globalisation and connectedness of all the organisations will put the human firewall not only to the front desk of an organisation but to all small enterprises that are suppliers or business partners to a securely better aware larger organisation.

In many cases when we succeeded in improving the human firewall of our organization and we have raised enough awareness it would not matter if the malicious attachment of an electronic mail message would bypass our firewall encrypted, because the employee who would decrypt it would be cautious not to open it unless it would be digitally signed or the file extension would not be showing that it could be a worm or a Trojan horse. The employee would know exactly how to react if an incident would occur, whom to report and what are the next steps. The notion of involvement means also higher employee satisfaction and thus less probability of internal attacks of employee sabotage.

4 The Requirements For eSecurity Implementation

Top management involvement in the strategy of an organisation is crucial. When it comes to involvement of top management in e-strategy there is usually less involvement. As long as there are not problems and everything seems to be running smoothly management normally does not consider e-security strategy and want to spend money or time on information security. However, only with high level commitment of management to introduce e-security as a part of the e-strategy in the process where all the employee will be involved we can expect to achieve desired success.

By appointing all employees and not only system administrators to be responsible for security in the company we can improve the overall level of security (Caminada et al, 1998, p. 429). Beside that we still need a person, also called information security officer, who is managing the overall information security process and would be controlling and managing the implementations of security policies and procedures. It is not uncommon to ensure the adequateness of a person by doing background criminal checking or asking the person to provide some proofs of their strict adherence to the law in the past.

The success of information security policy and the work of information security officer strongly depend on the support and encouragement of the top management, which should approve and determine the duties and responsibilities of the information security officer. The main roles of the information security officers would be daily management of the information security process. His roles would also include encouraging users to increase their information security awareness. Many times it is important to do introduction security training for all new employees. One of the most security (Caminada et al, 1998, p. 429).

Beside that we still need a person that would be in charge of e-security implementation within and organisation, also called information security officer or chief security officer, who is managing the overall information security process and would be controlling and managing the implementations of security policies and procedures. It is not uncommon to ensure the adequateness of a person by doing background criminal checking or asking the person to provide some proofs of their strict adherence to the law in the past. The role is certainly not an easy one, he must be familiar with technological, organisational and even legal aspects of e-security.

As in previous cases the success of information security strategy and the work of information security officer strongly depend on the support and encouragement of the top management, which should approve and determine the duties and responsibilities of the information security officer. The main roles of the information security officers would be daily management of the information security process and ensuring that the security posture of the organisation is accordant with the e-strategy. His roles would also include encouraging users to increase their information security awareness. Many times it is important to do introduction security training for all new employees, but also regular training for all the employees.

5 Conclusion

When acting on security issues organisations are mostly not proactive. Any problems that might arise are solved on an ad-hoc basis. What an organisation really needs is to have a well-defined and documented security policy in order to make sure most security issues are addressed. The security policy needs to have clear guidelines to inform all users about their responsibilities (Wen and Tarn, 1999).

Once appointing information security officers or chief security officers it is still too often undefined what their responsibilities are. Responsibilities should be clear and supported by the top management. All those responsibilities should be then documented and easily available to all employees throughout the intranet of a company. By doing this we are tackling only some parts of information security issues.

Solving the e-security problem is almost impossible in isolation. Without knowing the value of our assets it is nearly impossible to make rational decisions about appropriate protection mechanisms. However, securing the information systems and networks is useless if we are not dealing with other aspects of overall security posture, such us personnel security, physical security or even home security. The e-strategy of new global organisations will certainly include e-security in the future.

References

Anderson A., Longley D., Kwok K. (1994): Security Modelling for Organisations. ACM Press, New York, USA, p. 241-250.

Arhar F. (2000): SKLEP o dopolnitvi sklepa o določitvi pogojev, ki jih mora izpolnjevati banka oziroma hranilnica za opravljanje bančnih oziroma drugih finančnih storitev. 23.05. 2002 [Url:http://objave.uradni-list.si/].

Avolio M. F. (1998): A Multi-Dimensional Approach to Internet Security. ACM Networker Magazine, May 1998.

Barman S. (2002): Writing Information Security Policies. New Riders, Indianapolis, USA.

Bainbridge D. (2000): Introduction to Computer Law. Longman Pearson Education, Harlow, England. 478 pp.

Broderic J. S. (2001): Information Security Risk Management – When Should It be Managed? Information Security Technical Report, Volume 6, No. 3, pp. 12-18.

Caminada et al (1998): Internet Security Incidents, a Survey Within Dutch Organizations. Computers & Security, Vol. 17, No. 5, pp. 417-433.

Dhillon G. (2001): Challenges in Managing Information Security in the New Millenium. Idea Publishing Group, London, 184 p.

ISO/IEC 17799 (2000): Information technology – Code of practice for information security management.

Kolšek M. (2001): Penetracijsko preizkušanje informacijskih sistemov. Penetration Testing Information Systems.

Parker D. (1998): Fighting Computer Crime. A New Framework for Protecting Information. John Wiley & Sons, New York, USA.

Potter et al (2002): Information Security Breaches Survery 2002, PricewaterhouseCoopers, UK.

Samuels M. (2002): Good security policies should be second nature. Computing, 28. march 2002.

Schneier B. (2001): Managed Security Monitoring: Network Security for the 21st Century, 20, pp. 491-503.

Wen J. H. and Tarn M. (1999): Internet Security: a case study for firewall selection. Information Management & Computer Security 6/4, MCB University Press, pp. 178 – 184.

Yapp Peter (2000): Who's Bugging You? How Are You Protecting Your Information? Information Security Technical Report, Vol. 5, No. 2, pp. 23-33.