NETWORK SECURITY INVESTMENT

Mathews Z. Nkhoma, Hamid Jahankhani
Innovative Informatics research Group
hamid.jahankhani@uel.ac.uk

Abstract: Analysing potential risk and the allocation of resources for computer network security and business continuity require strategic, long-term planning. Most companies tend to be reactive and respond with quick infrastructure solutions. The purpose of risk analysis should be to assist managers in making informed decisions about investment and developing risk management policies. High countermeasures expenditure on every aspect of an information system is out of question in a commercial organisation. Therefore, this expenditure must be directed to reduce corporate exposure to information system risks in the context of overall business risks. The aim of this paper is to report the on going research to justify funding for network security expenditure through risk assessment practice.

1. Introduction

The advent of information technology has changed the face of doing business. The public and private sectors increasingly depend on information and telecommunications systems capabilities and services. In the face of rapid technological change, public and private organisations are undergoing significant changes in the way they conduct their business activities, including the use of wide area networking via public networks. These changes include mandates to reduce expenses, increase revenue, and, at the same time to compete in a global marketplace.

The needs for a reliable security network was also heightened by the issue of cyber-crime, which involves hacking into computers, creating and spreading computer viruses, perpetrating online fraud schemes, and stealing trade secrets and other intellectual property, (Potter, 2002). While some readers may think that e-security warnings are pointless and overstated, the reports of the computer Security Institutes' 2002 Computer Crime and Security Survey reveals that "90% of respondents detected computer security breaches within the last 12 months, 80% suffered financial losses due to computer breaches" (Kolodzinski, 2002:a). It was also gathered that the financial losses was brought about by financial fraud and theft of propriety.

Advanced level of network security provides maximum network flexibility as well as an additional layer of protection against unauthorized computer access. Moreover, this advanced security level also makes possible an audit trail of network usage. Another benefit is that a user authorization can be quickly and efficiently rescinded from the network.

Analysing potential risk and the allocation of resources for computer network security and business continuity require strategic, long-term planning. Most companies tend to be reactive and respond with quick infrastructure solutions, (Fratto, 2003).

There has been a reluctance to tackle the subject of risk due to perceived complexity and inexactness and therefore handle risk analysis and risk management effectively. This has led to a situation where many information systems do not even retain even the simplest risk management techniques,

which were present in the paper systems that they are replacing. Clearly with growing importance of information systems in all aspects of corporate operation, information systems must be made subject to appropriate risk analysis and risk management disciplines.

In case of computers and communications, the countermeasures that can be employed to reduce risk are well known and an array of techniques has been available for some time. High countermeasures expenditure on every aspect of an information system is out of question in a commercial organisation. Therefore, this expenditure must be directed to reduce corporate exposure to information system risks in the context of overall business risks. In particular, risk analysis must be able to answer the following questions;

- How much is it appropriate to spend on countermeasures?
- Where this spending should be directed?

One of the areas where spending in information systems can be directed is network security.

The information held on the organisation network plays a vital role in the organisation day-to-day business. But, knowing this is often not enough to convince middle or senior management that network security is important business issue.

In order to raise the profile of network security as a business issue, the value of information as a business asset and the cost of security breaches must be appreciate and what is needed is some solid quantitative evidence.

There are many insecure systems in operation and also there are many systems with inappropriate and over expensive security countermeasures, which are just as responsible for losing money, (Pricewaterhouse Coopers, 2004).

2. Network security as a business issue

Many organizations run on information, and a well-planned network circulates this information life-blood to all parts of an organization as efficiently as possible. The ability of a network to blend an advanced level of security with maximum operating flexibility, therefore, must be considered carefully in any network plans.

Unprotected information and computer networks can seriously damage a business's future. This happens because of the loss of classified or customer critical information, exposure of trade secrets, unacceptable business interruption, or lawsuits stemming from security breaches. As information and computer network security involves more than technology, companies are now spending more money and man-hours than necessary on cutting-edge technology. Inaccurate analysis of the company's needs can result in greater risk of information loss and higher frequency of security breaches.

Kolodzinski (2002b) presents potential grim scenarios for companies if they do not emphasize the importance of network security. Unprotected information and computer networks mean loss of data that are deemed crucial and confidential for the company's own development; loss of confidential third-party data; and business interruption or slowdowns that significantly impact the business as well as other parties. Kolodzinski (2002b) further stresses that any of these scenarios could result in loss of competitive advantage, lawsuit exposure, and unacceptable downtime (business interruption).

Threats against corporate data still continue to rise. More companies are storing increasing amounts of corporate data on information systems. Today, senior management express concern over the

threat, but has done very little to counter the threat. Senior managers fail to see information security as "value-added" contribution to "bottom line." It is true to say in 2004 the treat still is continuing to rise, because of the ever increase of inferences between IT and IS technology.

Senior managers are becoming more and more aware of the need to address security and information technology investments within the context of the corporation's business goals. As Schwartau (1997) has observed, Security is no longer just about security. Today, security is about resource and information management and it turns out that good security is a by-product of a well-run organization.

Information systems (IS) executives are most concerned with ensuring that their technology goals are consistent with those of the overall business, believing that an effective organization and usage of the company's data is a critical IS activity.

Williamson (1997) suggests an approach to setting priorities for IT projects and some criteria for IT investment decisions that are potentially applicable to information security investment decisions. This approach consists developing a formal, quantitative way to assess the business value of proposed projects; engaging customers in a dialogue about the available resources and business needs throughout the year, not just at budget time; interviewing customers about their wants and needs; communicating frequently with customers about the Information Security (IS) department's achievements, current projects and short-term plans.

Williamson (1997) also considers the importance of remembering the human element; take egos and the need for validation into account; working with committees structured to minimize the influence of any one individual or department; visiting with the business units; communicate clearly how priorities are set so that people can anticipate project funding decisions; and developing a business case for every project, assessing its risks, its business value, and the cost of building or buying it. Additionally, the said author' approach calls for the demonstration of interest in the constraints under which business customers operate, and staying on top of changes in the regulatory and competitive environment in which the business operates. Here, it is emphasized that decision-makers must be prepared to show how a proposed project fits with business goals. According to Kolodzinski (2002b), the primary goal then is to develop a scalable corporate security structure that is responsive to short- and long-term needs as well as shifts in technology. By knowing future needs, security planners can anticipate requirements for information protection with a view to making them able to expand or contract according to strategic actions that the company takes in pursuit of its targets and goals.

3. Risk assessment

Information systems have long been at some risk from malicious actions user errors and from natural and man-made disasters. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or hacking techniques are becoming more widely known via the Internet and other media.

Although all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. In particular, risk

assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organisations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected.

It is worth taking time to explore just why the Internet has completely changed risk management landscape. By its very nature, the accessibility and relative anonymity of Internet users make internet based systems (and the integrity of the information stored on them) constantly vulnerable to security threats.

It should not be assumed that protection against risk is achieved by throwing up massive fortifications around the information system installation. It is more important to select exactly the right countermeasures, targeted at the risks which matter most. The desire to control and protect information is rooted in the notion that information has a value. But how can this value be assessed? In summary, exact valuations of information systems and their contents are difficult because;

- Value is not necessarily related to acquisition or development costs;
- Perceptions of value will vary widely among different users of the same systems;
- Value often depends on transient qualities, such as timeliness and relevance;
- For information internal to the firm, values cannot be market tested.

An organisation cannot hope to develop effective data security measures unless first of all has a clear idea of what it is trying to protect itself against. It should be stressed that threats to data do not necessarily arise from a deliberate intention to cause damage. A threat in this context is defined as any potential source of harm to the reliability or integrity of the information technology system. The threat may originate through ignorance, incompetence, carelessness, malice, or a combination of these factors, (Wakefield, 2004). It is also important to anticipate potential failures due to weaknesses built into the system, which can be triggered quite innocently. In other words, the system itself is in a state which safety analysts would regard as constituting a hazard. Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations, outcome and make informed judgements concerning the extent of actions needed to reduce risk.

4. Business risks

Being in business is a risk. For most commercial organisations, the value of the information associated with the network security greatly exceeds the value of the technology associated with it (unless the IT strategy of the organisation is inappropriate). There are cases that the value of the technology assets is known to be near seven significant figures (because they appear on balance sheets) whereas the value of the information assets is not known to the nearest order of magnitude. Proper business investment decisions cannot be made in such an environment. The objective of risk management is to reduce business exposure by balancing countermeasure investment against risk. It may be that the countermeasure expenditure would be better directed to other parts of the organisation. If this is the case, then risk management should confirm this. It is important to remember that the purpose of risk analysis and risk management procedures is not

simply the definition of countermeasures. Risk analysis and risk management must be part of the ongoing operations of an organisation but within that organisation should be no more or less important than any other disciplines associated with network security.

Risk analysis is a technique for quantitative assessment of the relative value of protective measures. Classical risk assessment is a process that quantifies losses. In building any business case for network security, it is vital that a return on investment (ROI) is shown. Quantitative risk assessment allows putting real figures on potential losses to justify the costs of implementing network security. According to (Kaplan, 97) risk can be defined as three questions: (1) what can happen? (2) How likely is it? And (3) what are the consequences? Answering these simple questions helps quantify risks. Risk analysis is a method of quantitative assessment of relative values of protective measures and the Annual Loss Expectancy (ALE) is the projected costs for identified risks. Before the Internet, information security had rarely been perceived as a critical success factor for modern business. In fact, the opposite is true. Information security was relegated to cost centre, status, and little impact on the financial goals of an enterprise. For management and staff alike, initiatives to improve security resulted in additional paperwork, signatures, and calls to the help desk. The Internet helped to change that. Security is starting to be perceived as an enabler, a tool to safely open the doors to the Internet and electronic business, (Muraca, 2004).

5. Analyzing returns on security capital investments

When compiling data for an IT security investment proposal, it can be challenging to deliver one of the most basic capital-budgeting requirements: quantifying returns of events not happening, while using objective figures to support the business case. Fortunately, information collected in the annual CSI/FBI survey can serve as independent, impartial, and reliable data that can effectively illustrate potential costs and associated vulnerabilities inherent in under-security.

Choosing an acceptable and representative evaluation tool is the next challenge the IT executive faces, below are some of the appropriate analysis tools;

- Net present value
- Internal rate of return
- Return on investment
- Payback period
- The bottom line

It is important to note that there are other models that can be used, such as economic value-added and option models.

Conclusions

Effective IT budgeting must relate the available funds to the expected returns and should take into account not only the investment and resource requirements of all IT initiatives on a project by project basis but also the capacity of the organization to undertake the work.

Thus the research will provide a solution which offers a customizable, guided process for constructing a performance-based budget, which can be as simple or as sophisticated as required to fit the needs of the organization. The required budget can then be built on a project and asset basis, and funds can then be built on a project and asset basis, and funds can then be allocated from different departments or other funding sources.

Risk exposure is measured as the productivity loss due to existing security

issues. Solutions are presented that minimize this loss and therefore provide instantly reliable returns, as opposed to returns that only happen if the security solution prevents a major disaster. Solving these problems provides real returns and improves security at the same time, which has the side-effect of preventing some of those major disasters.
Not only is productivity a major factor in calculating risk exposure, it's also a significant factor in the cost of a solution. Security solutions can have a positive, negative or neutral influence on organizational productivity. This influence can be significant and must be factored into the cost of the solution.

References

Fratto M. "Don't Panic. Plan." Network Computing website. http://www.networkcomputing.com/1408/1408f1.html. May 1, 2003.

Kaplan, S., Words of Risk Analysis, Risk Newsletter, 1st Quarter, 1997, pp8,9.

Kolodzinski, O., 2002a, Cyber-Insurance Issues: Managing Risk by Tying Network Security to Business Goals, The CPA Journal, 72(11), 10+.

Kolodzinski, O, 2002b, Aligning Information Security Imperatives with Business Needs, The CPA Journal, 72(7), 20.

Muraca D., Technology Risk Services, Price Waterhouse Coopers, 2004.

Potter, G., Business in a Virtual World: Exploiting Information for Competitive Advantage, Houndmills, 2002, UK, Macmillan.

Pricewaterhouse Coopers , 2004, Information Security Breaches Survey 2004, Technical Report, UK, Department of Trade and Industry http://www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf. April 2004

Wakefield, R. L. (2004). "Network Security and Password Policies." The CPA Journal, 74(7), 6.

Williamson, M., 1997, Weighing the NO's and CON's CIO, April 15, 49.