Author(s): Nkhoma, Mathews Z.; Jahankhani, Hamid; Mouratidis, Haralambos.
Title: Information and network management security Investment
Year of publication: 2007
Citation: Nkhoma, M.Z.; Jahankhani, H.; Mouratidis, H. (2007) 'Information and network management security Investment' Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 2nd Annual Conference, University of East London, pp.89-100
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/ACT07.pdf

Information and network management security Investment

Mathews Z. Nkhoma, Hamid Jahankhani, Haralambos Mouratidis
Innovative Informatics Research group, School of Computing and Technology

Abstract: In today's business environment it is difficult to obtain senior management approval for the expenditure of valuable resources to "guarantee "that a potentially disastrous event will not occur that could affect the organisation performance. 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. A strategic approach to computer network security leads to a more efficient plan and a less expensive risk-management strategy. Financial modelling is a fundamental component of all business investment cases. IT security investment proposals have unique qualities that can pose expenditure justification challenges. This paper aims to explore various financial models and to develop one that IT managers can effectively use to support their business cases.

1. Introduction:

The business risk for a company engaged in technologically dependent business is normally greater than for one that is not. Business operations present a unique set of risks, including an increased reliance on technology and increased vulnerability to the rapid changes in technology. In addition, industry structures can erode rapidly because Internet shopping facilitates price competition and transforms core business structures to promote distribution by mail and remote customer service. To address such challenges, a company or a certain organisation needs to develop an effective strategy. An effective strategy requires operational efficiency; within organisation's information systems, this means an emphasis on information security and controls. A cost-effective business internal control system should be designed and implemented toward the goal of reduced operating expenses and therefore increased profits. Reducing operating expenses and increasing profits are critical to the success, even the continued survival, of companies heavily engaged in business.

Computers have found their way into all areas of business, industry, education and government. Increasingly far reaching information networks linking computers and databases provide important benefits, including greater staff productivity and a sharper competitive edge. The more that we expand the reach of our information networks, the more important network security becomes. Basically, this paper discusses the relevant issues about security particularly the security in information management and network management.
Financial modelling is a fundamental component of all business investment cases. IT security investment proposals have unique qualities that can pose expenditure justification challenges. This research is designed to explore various financial models and to develop one that IT managers can effectively use to support their business cases.

2. Information security management:

An effective information security program incorporates a combination of

technological and human controls in order to avoid the loss of information, deter accidental or intentional unauthorised activities, prevent unauthorised data access, detect a loss or impending loss, recover after a loss has occurred, and correct system vulnerabilities to prevent the same loss from happening again (Jahankhani and Nkhoma 2004). Correspondence among businesses, internal or external, is conducted through data transmissions. Data transmissions pass in networks of interconnected portals where parties could get in touch with one another. Networks need to be protected from both outsiders such as hackers and crackers, and insiders such as employees and other individuals with access to the network. The industry defines hackers as individuals with extensive computing knowledge that look for internal and external system holes, some for fun, and others for a purpose. Crackers are individuals that try to break into a system by guessing or cracking user and system passwords.

In a world where hackers, computer viruses and cyber-terrorists are making the headlines daily, security has become a priority in all aspects of life, including business. But how much does a business become secure? How much security is enough? How much does a business know when its security level is reasonable? Most importantly what's the right amount of money and time to invest in security?

Making computer and communication systems more secure is both a technological challenge and a managerial problem. The technology exists to incorporate adequate security safeguards within these systems, but the managerial demand for secure systems is virtually nonexistent outside of the defense and financial industries. That so many of our commercial systems provide marginal security at best is a reflection of the lack of managerial awareness and understanding of the need to protect the information stored in, and transmitted between, computers. The economic ramifications of inadequate security can be significant. To illustrate, Volkswagen lost almost $260 million as the result of an insider scare that created phony currency-exchange transactions and then covered them with real transactions a few days later, pocketing the float as the exchange rate was changing (Neumann, 2002). Similarly, The Bank of New York experienced a $32 billion overdraft as the result of a processing error that went unchecked. The bank had to borrow $24 billion to cover its transactions for one day, and paid $5 million for the day's interest (Neumann, 2001). Furthermore, when the government of India requested bids on a billion-dollar contract for jet fighters, French intelligence agents stole bid information submitted by the United States and gave it to a French firm competing for the contract. The proprietary information helped the French company to win the contract (Mello, 2002). Likewise, a group of hackers, operating under the name Masters of Deception, victimised such companies as Southwestern Bell, New York Telephone Company, Pacific Bell, US West, TRW Inc., Information America Inc., Martin Marietta Electronics Information and Missile Group, ITT Corporation, Educational Broadcast Corporation, Bugle Boy, New York University, and the University of Washington. The hackers stole credit reports, and altered or deleted files at some sites. Southwestern Bell alone reportedly spent $370,000 to repair corrupted programs and to buy more secure hardware and software (Kaplan & Clyde, 2003). Information security, right now, is a

confused and paradoxical business. For example:

- You've increased spending significantly, and you're told this is a good thing, and yet it has had zero effect in mitigating security breaches.
- You're constantly warned about "digital Pearl Harbors" and yet the vast majority of incidents you report are relatively small, don't last long and don't cost much.
- You're told that aligning security and business strategies is a top priority, and yet those who have fared best in avoiding breaches, downtime and security-related damages are the least likely to be aligned with the business. But in another sense, you seem to be contributing to the confusion.
- Respondents who suffered the most damages from security incidents were two times more likely than the average respondent to plan on decreasing security spending next year.
- Those with the most damages were nearly half as likely to list staff training as one of their top three priorities.
- A quarter of you neither measured nor reviewed the effectiveness of your information security policies and procedures in the past year.

In short, the survey shows that as much as the nascent information security discipline has grown since its baptism—on Sept. 18, 2001 (one week after the terrorist attacks and the day the Nimda worm Hit)—it hasn't much improved with age.

Network resources allow worldwide access to information, no matter where it resides, or where the users are located. Unfortunately, the physical and logical controls used by an organisation to secure its information offer no protection when that information is being electronically transmitted. In a survey, which included responses from 538 computer security practitioners in various institutions, contained some sobering figures that 85% of respondents detected computer security breaches in the last 12 months while 64% acknowledged financial losses due to the breaches. Similarly, it found out that 35% quantified their losses, a total of almost $400 million while 40% detected system penetration from the outside. Its findings also reflected that 91% detected employee abuse of Internet access privileges while 94% detected computer viruses. (Niederhoffer, 2002)

Concomitantly, another survey found that U.S. businesses spent only 0.02% of their top-line revenue on data security and that 75% of business networks are wide open to hacking. (Mello, 2002) Although smaller companies seldom see themselves as targets, experts say attackers scan entire networks and view any site as fair game. A useful way to think of the Internet is as a series of smaller networks that anyone can access. Corporations or governments manage many of these smaller networks but no one has overall control. There are opposing views as to what role the government should play. Individuals outside of an organisation pose threats to communication security, and their attacks can be active or passive. Active attacks intentionally cause the transmitted information to be changed. An intruder could make undetected and unauthorised modifications to the contents of a transmitted message. Information may be deleted or delayed, or changes could be made to the order in which a series of messages are transmitted. The destination address of a message could be changed, causing the message to be directed to another party. Or the origination address could be altered, causing the receiver of the message to believe that the transmission was sent from a different source.

Legitimate messages could be recorded and later played back, allowing an unauthorised user to establish a connection under a false identity, or causing a transaction to be performed twice. Active attacks are easier to detect than to prevent.

Similarly, passive attacks result in the unauthorised disclosure of transmitted information. Passive threats to security arise whenever messages are intercepted and read by outsiders. (Kaplan and Clyde, 2003) In some cases, the mere existence of message traffic is important to an intruder because the pattern of messages may reveal the amount of business being transacted between different users. Passive attacks are easier to prevent than to detect.

With the emergence of technological advancements in data transmission among businesses, the installation of a security system has become a requirement. The network operating system (NOS) is typically the first layer of security in controlling user access from a logical security perspective, especially in a distributed system. The NOS controls the user identification, authentication, authorisation, and many security and permissions settings for all users and resources on the network. In user identification, the user tells the NOS who he or she is. The NOS authenticates the user by mapping user-supplied credentials, such as user IDs and passwords, to a centralised user store of networked systems. The NOS then authorises the user to perform various functions (such as read data, change data, delete data, or execute programs) based on stored user and group settings established by the network administrator.

Although individual application-level security usually controls what functions a user can perform within applications, poorly designed or ineffective NOS controls may allow data to be manipulated outside the applications, thereby violating the confidentiality, integrity, and availability of the underlying information. (Rogers and Freiberg, 1994) However, failure to consider NOS security controls may lead to unfounded reliance on the application, reconciliation, and monitoring controls. The general computer controls review should include an assessment of the controls surrounding the NOS. Such testing would examine applicable service packs and security updates installed, system configurations, and network connections.

Moreover, unauthorised access to data is a major risk faced by enterprises. News groups, discussion forums, and best-selling books such as Hacking Exposed (McClure et al. 2001) have made it relatively easy to gain unauthorised access to corporate information resources. Therefore it is imperative for organisations to keep abreast of patches, updates, and proper system settings. To ensure adequate controls at every level of the information technology infrastructure, public accounting firms and corporate internal audit divisions are increasingly hiring information technology specialists.

In this light, organisations could safeguard their data and decrease the possibility of losses and distortions during transmission by several measures. An organisation could use network-monitoring software. Such software monitors the data flow and detects weak points--hardware configurations or software arrangements that are likely to cause transmission errors. Organisations could also upgrade to conditioned telecommunication lines. Because such lines are cleaner in producing less static and other encumbrances in transmission rates that can be boosted without errors, resulting in lower transmission costs. Fiber optic lines offer the most advantages in

data efficiency and security; they are capable of carrying enormous volumes of data at high speeds with little or no distortion, and they are almost impossible to tap. Fiber optic lines, however, are not yet widely available. Similarly, the application of protocol controls is also required. In a typical situation, software monitors the transmission reliability by directing the receiving and sending software to acknowledge the transmission link, then agree on a transmission protocol and finally verify the accuracy of the data transmitted. Likewise, the enforcement of backup and recovery procedures is essential. No network is fail-safe. As a network design becomes more sophisticated, the probability increases that at least some part of it will fail. Backup and recovery procedures provide contingency planning for network downtime and include securing alternate network facilities, planning for alternate means of data transmission and eliminating confusion over what data were preserved in instances of transmission interruption. More importantly, the use of network access controls is deemed necessary. Determined hackers can break into almost every computer network. Any organisation without access controls--passwords--is inviting trouble. Depending on the organisation, passwords should be assigned to every user at various levels of the operation. In some cases, this may even mean assigning selective access to specific computer files.

3. The Way Forward:

Before spending money on a security product or service, most decision makers will want to know that the investment is financially justified. There's no point in implementing a solution if its true cost is greater than the risk exposure.

Setting the IT budget is often an unstructured exercise with a lack of recognized methodology and no link to strategic goals of the organization. The outcome is often a proposed budget that bears little relationship to business requirements and value.

In order to determine how much should be spent on security a decision maker needs to know:

- How much do existing security problems cost the business?
- What impact would a catastrophic security breach have?
- What are the most cost-effective solutions?
- What impact will the solutions have on the business?

Financial modelling is a fundamental component of all business investment cases. IT security investment proposals have unique qualities that can pose expenditure justification challenges. This research is designed to explore various financial models and to develop one that IT managers can effectively use to support their business cases. Determining costs incurred as a result of specific attacks should seem simple enough to do, but typically many intangibles are involved and costing analyses can prove somewhat challenging.

The CSI/FBI statistics can provide reliable measuring points, but IT managers can use alternative methods when developing a business case for network security. Single-loss expectancy (SLE), annualized rate of occurrence (ARO), and annual-loss expectancy (ALE) can be effectively used when attempting to place value on an event that did not occur. This paper looks at these in detail.

3.1. Single-Loss Expectancy;

The single-loss expectancy (SLE) is the cost associated with a single attack on a specific asset. SLE is typically determined by multiplying an asset's value (for example, the value of a server) by its exposure factor.

The formula for calculating SLE is SLE = Asset value*Exposure factor

Asset Value

Asset value can be challenging to estimate. In the example of a web server, you must determine whether the asset value represents the data or simply the media in which it resides.

The asset value could be represented by the formula shown as;

Cost of replacing information + cost of replacing software and hardware and reconfiguration + lost availability + associated costs (loss of data confidentiality and integrity) = Total Asset Value

The asset value cost would vary depending on the kind of attack that had occurred. A DoS attack, as an example, would typically not involve hardware replacement, whereas an outright theft of a server would include many possible variables, such as costs associated with loss of confidentiality and integrity.

Exposure Factor

An exposure factor illustrates an asset's vulnerability to a given threat. It measures the magnitude of a threat's impact on a particular asset and determines a percentage of the asset that would be lost should a particular type of threat occur.

An IT manager can attempt to estimate the total costs surrounding a single attack, or can instead choose to pull information from an array of different sources. The CSI/FBI information has been discussed, but other governmental and institutional agencies gather information as well, including the UK Department of Trade and Industry (DTI) Information Security Breaches Survey 2004, published by Pricewaterhouse Coopers (PWC) and the DTI.

Depending on system resources and time availability, using third-party data can ensure greater credibility and speedier compilation when developing a business case.

3.2. Annualized Rate of Occurrence:

The annualized rate of occurrence (ARO) is the probability, or rate, that an attack might happen over a one-year period. Statistics can be excellent tools, provided that sources are reliable. The CSI/FBI determined, as an example, that 36% of its respondents had been victims of system penetration attacks in 2003.

Note that at times, statistics from different sources can appear to be conflicting. In organizational environments that are focused on prevention, it is prudent to be on the side of caution while continuing to study the trending.

Also it should be Noted that, exposure factor is often represented as a decimal value, whereas ARO is usually represented as a percentage.

3.3. Annual-Loss Expectancy:

With SLE estimates and ARO statistics completed, the annual-loss expectancy (ALE) can be calculated. The formula used is shown below. The ALE can be used in a capital-budgeting process whenever an organization is considering an equipment investment proposal. Relevant attack costs can be determined in-house, or organizations can comfortably use external information culled from a wide cross

section of industry and government on the North American and European continents.
The formula for ALE is;
single loss expectancy (SLE) * annualized rate of occurrence (ARO) = ALE

4. Budgeting for Security Equipment:

The next step in the business case is to develop a cost model for the equipment that is designed to protect an organization from attack.
This area explores the cost of equipment, as follows:

- Total cost of ownership
- Present value

4.1. Total Cost of Ownership:

The total cost of ownership (TCO) includes all associated equipment costs, whether recurring or nonrecurring, including all aspects of hardware, installation, maintenance, and upgrades.
If other costs are pertinent to an organization, such as ongoing training, as an example, they should be included in the final model. Depending on the organization and the level of analysis expected from those who prepare the metrics, additional TCO variables could include the cost of floor space, insurance, utilities, and so on.
Because many factors can affect overall calculations, including, but not limited to, amortization period or whether the equipment is being rented or leased, you are encouraged to gather as much data as possible before compiling this portion of the model.

The total cost of ownership can be calculated as;

TCO = P+N+(Y*R)
Where:

P=procurement cost
N=Non-Recurring costs
R=Recurring costs
Y=useful life of the equation in years

4.2. 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, and this section aids in the search of an appropriate analysis tool by exploring the merits of the following topics:

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

It is important to note that while other models can be used, such as economic value-added and option models, the discussion in this paper is best served by focusing the analysis on the four methods covered in this section.

4.3. Net Present Value:

Net present value (NPV) provides a dollar value for a future return brought back to

present time. It is calculated by adding the present value of benefits, for every year over a specified time period, and then subtracting the initial recurring and nonrecurring costs of the investment. A positive NPV represents a profit, while a negative NPV signifies a loss.

4.4. Internal Rate of Return:

Internal rate of return (IRR) can be viewed as a sort of go/no-go decision level for an investment proposal. IRR is often used to analyze investments that span over many years. IRR is similar to NPV in that IRR equals the discount rate by which the net benefits must be discounted, over the time period, until the point that they equal the initial costs.

4.5. Return on Investment:

Return on investment (ROI) is a reliable tool that is widely used to compare the attractiveness of various business investments. ROI equals the present value of the net benefits over the useful life of the proposed equipment, divided by the TCO of the equipment. It is usually expressed as a percentage over a specific amount of time; three years is a common time span for IT equipment. The ROI formula is;

$$ROI = \frac{PV\ Savings - PV\ TCO}{PV\ TCO}$$

4.6. Payback and the Bottom Line:

While payback is simple to calculate, its drawback is that it does not sufficiently illustrate the magnitude of the savings, nor does it highlight any benefits the investment could provide after the break-even point.IT security is a relatively young industry. Most established industries have a wealth of act upon data that has been collective over decades. The security field relies on recent data, culled from concerned IT and business professionals who cut a wide swath across industry and government and whose common goal is to create a forum for sharing this pertinent data.

IRR and NPV bring unequalled value to financial modelling, but given the specific nature of IT security investing, it is the view of the authors that ROI, or return on security investment (ROSI), is the most appropriate vehicle to ensure the effective development of an informed and substantive business case for network security. But no single method is perfect for assessing security capital budgeting. What cannot be disputed, whether the source is CSI/FBI, PWC-UK, or any other well-regarded resource, is that cyber-crime is on the rise, and the risk to industry, both in dollars and reputation, must be measured by every organization before any long-term plan can be put in place.

5. Acknowledging Nonmathematical Security Fundamentals:

Much of the discussion in here has centred on why, how, where, and what to secure. But the question of when to secure is somewhat more elusive. Financial modelling can dictate that the time for security is when it is financially feasible. Managers might say that the time for greater security is when something is relevant to secure. But much of what is protected in IT security is not always tangible, for example, customer relationships, trust, goodwill, and the sanctity of data that supports each entry on a financial statement.

Organizations are highly exposed to the vulnerabilities inherent in Internet connectivity, and the exposure increases every day as viruses become more virulent and users neglect to exercise ever-greater caution. Moving away from the Internet is

not an option for most organizations. Competitiveness demands an ever-increasing presence, and therefore reliance, on all things electronic. But many organizations have grown much larger by using their reliance on the Internet, as the face of business transactions has changed dramatically over the last generation.

In her article in iQ magazine, Kathy Harris identifies ten categories of potential value that businesses can realize by virtue of being connected to the Internet: from quick time to market, new revenue streams, improved customer service, and greater process effectiveness to the creation of intellectual capital, greater asset utilization, and better connectivity with partners and vendors. The argument is made that softer benefits resulting from the newfound reliance on the Internet are difficult to quantify, yet going backward cannot be an option. She goes on to state that, ". . . creating value propositions always requires a certain amount of qualitative judgment.

The financial modelling in this paper should be fully used and effectively presented. But in the end, IT security is far greater than the mere sum of its parts.

In order to answer these questions, measurement tools that show how security problems and expenditures impact the bottom line are needed. The Holy Grail of security, from business point of view, is to be able to calculate a return on investment (ROI) for any security expenditure. The search of an effective way to measure ROI for security has lead to a number of interesting models, none of which have yet been accepted as the standard methodology.

ROI and ROSI defined

ROI is a simple yet powerful concept. 'Which of these options gives me the most value for my money?'-that's the fundamental question that ROI is designed to answer. ROI is frequently used to compare alternative investment strategies. To calculate ROI the cost of a purchase is weighted against the expected returns over the life of the item. A blended attack hit.

Managers responsible for computer security are increasingly required to justify their budget requests in purely economic terms. There has been considerable discussion of economic metrics used to justify and evaluate investments in computer security at trade and academic meetings, as well as in computer security journals.

In the case of security the expected return is often interpreted as the amount of money that company will save from not having security problems as a result of the investment. This is because security investments usually don't create value-they simply prevent bad things from happening. The cost of a bad thing happening is called risk exposure. A security solution mitigates that risk by some percentage. Multiplying the exposure by the percentage mitigated gives the expected return.

The trick with return on security investment (ROSI) is in figuring out the expected returns and the true cost of the investment. Determining expected returns for security investment involves estimating the risk exposure and the amount a solution will mitigate the risk, neither of which is easy.

The inability to predict the total cost associated with security incidents can be sidestepped if we can find a single cost component that; can be consistently measured, strongly correlates to the overall cost or is significant in its own right.

Make such a health check broad in order to capture risks associated with every stage of a programme. Areas for consideration should include, but not limited to:

- Commercial arrangement with suppliers
- Organizational issues (roles, responsibilities, skills, resources);
- Project planning
- Change management
- Requirements definition
- Design
- Build
- Configuration management
- Test and acceptance
- Quality strategy
- Risk management strategy
- Go live and cutover plans
- Licence agreements
- Support contracts
- Technical evvironments
- Physical and electronic security
- Business processes and continuity
- User tranning
- Failover and redundancy

Key questions in each of these areas produce an immediate and accurate picture of a programme's health. Once this health status has been determined the correct course of treatment can then be prescribed. Output from a health check activity should be a comprehensive risk register, with risks classified in terms of both the likelihood and impact of occurrence. The register can then be used to focus finite programme resources on those risks that fall outside an organization's level of tolerability.

It is our opinion that a security incident's impact on productivity makes for an ideal cost component that suits all three conditions. Most important by using productivity as the exposure component of ROSI, security projects that improve business efficiency are prompted and those projects justified solely by fear of the unknown are eliminated. A meaningful ROSI can be calculated by focusing on the impact security has on productivity.

6. The relationship between productivity and security:

The productivity lost due to security incident can have a serious impact on the bottom line. For many organizations the cost of lost productivity associated with a security incident is far greater than the cost of data recovery or system repair. Productivity is not only a factor in risk exposure-it's a factor in the cost of a solution as well. Because security almost always comes at the cost of convenience, most security solutions end up creating hurdles that employees need to jump in order to do their jobs. Depending on the size and frequency of these hurdles, the lost productivity cost can seriously add up. The situation doesn't have to be grim it is possible for security solutions to increase productivity, (Udo, 2001). This happens when side-effects of a solution eliminate other significant problems that were hampering productivity. For example implanting a firewall might require network restructuring. The new structure might solve serious bandwidth problems that were previously creating extensive downtime. With good planning most security solutions can be implanted in a way that results in an overall enhancement of productivity. The cost of a solution must include the impact of the solution on productivity, since this number is often large enough to make or break the viability of a given solution.

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.

Organizations are highly exposed to the vulnerabilities inherent in Internet connectivity, and the exposure increases every day as viruses become more virulent and users neglect to exercise ever-greater caution. Moving away from the Internet is not an option for most organizations. Competitiveness demands an ever-increasing presence, and therefore reliance, on all things electronic. But many organizations have grown much larger by using their reliance on the Internet, as the face of business transactions has changed dramatically over the last generation.

The Holy Grail of security, from business point of view, is to be able to calculate a return on investment (ROI) for any security expenditure. The search of an effective way to measure ROI for security has lead to a number of interesting models, none of which have yet been accepted as the standard methodology.

The research is the real world implementation of the concepts put forth in this discussion. Its goal is to provide a trustworthy standard for security benchmarking, one that produces consistently repeatable results which are strongly correlated to financial performance. The unique approach taken by this document is its focus on productivity. Risk exposure is measured as the productivity loss due to existing security issues. Solutions are to minimize this loss and therefore provide instantly reliable returns, as opposed to returns that only happen if the security solution prevents a major disaster.

The assumption is that serious disasters are rare and hard to quantify but everyday incidents create a significant amount of aggregate loss. 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. The paper can estimate the impact a given solution will have on overall productivity. This impact is factored in when prioritizing underlying problems and their respective solutions. The analysis indicates the top problems prioritized by their impact on risk exposure and lost productivity. Likewise the solutions presented are selected based on their predicted ability to mitigate risk and minimise lost productivity. The result is the only automated, repeatable and consistent ROSI benchmarking system available to date. By far after implementing the project the organization can have the following benefits:

- Increase online sales
- Enhance customer satisfaction
- Improve ROI
- Protect reputation
- Maximise your reach
- Ensure availability
- Maximise customer retention

References:

Jahankhani, H. Nkhoma, M.Z. (2005), "Information Systems Risk Assessment", international Conference on information and Communication Technology in management, 2005, Challenges and Prospects, 23-25 may 2005, Malaysia.

Kaplan, R. and Clyde, R. (2003). "Learning from Loss: Classic VMS Security Breaches," InfoSecurity News, (May/June), pp. 28-29.

McClure, S., J. Scambray, and G. Kurtz. (2001) Hacking Exposed: Network Security Secrets and Solutions. Third edition. Berkley, CA: Osborne/McGraw-Hill.

Mello, J.P. (2002). "Espionage! Are the Spooks Targeting Your Business?" InfoSecurity Product News, (September/October), pp. 1-10.

Neumann, P.G. (2002). "Expecting the Unexpected," Communications of the ACM, (May), p. 128.

Niederhoffer, M. (2002) Internet Security and the CPA. The CPA Journal. Volume: 72: 8.

Rogers, C. R., and H. J. Freiberg. (1994) Freedom to Learn. Third edition. Columbus, OH: Merrill/Macmillan.

Udo, G.J., (2001) Privacy and security concerns as major barriers for e-commerce: a survey study. College of business administration, University of Texas (USA)