CERIAS Tech Report 2001-127

Value at Risk: A methodology for Information Security Risk Assessment

by J Rees, J Jaisingh
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Value at Risk: A methodology for Information Security Risk Assessment.

Jeevan Jaisingh and Jackie Rees
Krannert Graduate School of Management
Purdue University
West Lafayette, IN, 47907

Abstract

This paper presents Value at Risk (VAR), a new methodology for Information Security Risk Assessment. VAR summarizes the worst loss due to a security breach over a target horizon, with a given level of confidence. More formally, VAR describes the quantile of the projected distribution of losses over a given time period. Most of the tools that are used for ISEC risk assessment are qualitative in nature and are not grounded in theory. VAR is a useful tool in the hands of an ISEC expert as it provides a theoretically based, quantitative measure of information security risk. Using this measure of risk, the best possible balance between risk and cost of providing security can be achieved. Most organizations, especially those heavily invested in eBusiness, already have determined the acceptable level of risk. The dollar amount of this risk is then computed. When the total VAR of an organization exceeds this amount, the organization is alerted to the fact that an increased security investment is required.

I. Introduction

Information Security (ISEC) is an important function in organizations and several authors (Finne 1997; Bhimani 1996) have pointed out that breaches in ISEC can bring significant economic losses. The importance of providing an infrastructure for secure transactions for Electronic commerce has been emphasized in the security literature (Bequai 2000; Bhimani 1996). Information systems have long been at risk from malicious actions, inadvertent user error, natural disasters and other unforseen adverse events. In recent years, systems have become more susceptible to these threats due to the increasing interconnectivity of computer networks and, thus, more interdependent and accessible to a large number of individuals. Internet-based fraud is a growing global problem according to a recent survey. According to the survey, 83% of the merchants surveyed who sell goods online acknowledged that the threat of fraud is a serious problem (Bequai 2000). The consequences of losing sensitive information can be catastrophic. Media hyped reports of the "BubbleBoy" virus and frequent network failure of eCommerce sites like E*Trade may serve to alarm the public, but the threats are real (PFIRES 2000). The financial risks are alarming: In 1999 $7.6 billion was lost in business productivity by Melissa, the Worm and other viruses (Briney 1999). Previous approaches to security have concentrated on the technical aspects of security (Oppliger 1997, Bhimani 1996), models for security infrastructure (Sherwood 2000) and security policies (Finne 1998, Eloff 2000). However, there has been very little research done in the area of risk assessment and in figuring out the optimal level of information security and corresponding level of investment. Traditional investment decisions are made using cost-benefit analysis. Applying cost-benefit analysis to choosing the optimal level of security is tenuous at best due to the difficulty in measuring the benefits associated with increased security and in measuring the risk in terms of security. The

problem of developing an appropriate and useful methodology for risk assessment, and consequently choosing the optimal level of investment in information security will have to be addressed both by academics and practitioners, as ISEC investments are going to account for an increasing proportion of the total investments of an organization in the future. This paper proposes a new methodology for risk assessment, based on the Value at Risk (VAR) concept used in finance.

The paper is organized as follows: Section II presents the current state of affairs in ISEC policy and specifically focuses on risk assessment. In section III the VAR framework for Risk assessment is introduced and Section IV presents the conclusions, limitations of this study and directions for future research.

II. Background

According to Turban et al. (1996), risk is the likelihood that a threat materializes. Risk is to some degree unavoidable, so the organization must accept some degree of risk. Risk in any context is the sum of threats (those events which cause harm), vulnerabilities (the openness of an enterprise to the threats) and asset value (the worth of the asset in danger). An increase in any of these factors increases the risk (Finne 1998). Thus, in measuring risk associated with ISEC we need to measure the sum of threats, vulnerabilities and the asset values.

The aim of Risk Management is to identify, measure and control uncertain events, in order to minimize loss, and optimize the return on the money invested for security purposes (Caelli1989). Risk Analysis is a stage of Risk Management that focuses on minimizing the risk by effectively applying security measures commensurate with the relative threats, vulnerabilities, and values of the resources. Anderson et al. (1991) propose a three-staged methodology for Risk Analysis. The first stage of Risk Analysis is Asset Evaluation, the second stage is Threat and

Vulnerability Analysis, and the last stage is Safeguard Selection. The Asset Evaluation stage of risk analysis is fairly simple, since each organization has a fair idea of what its assets are. Threat and Vulnerability Analysis poses problems since there is no guarantee that the investment will provide adequate returns. According to Anderson et al. (1991), it would be nice if risk analysis always yielded a figure representing riskiness, such as "you would have an 89.5% chance of suffering an asset loss of $100,000 in the next year".

There have been some studies (PFIRES 2000, GAO 1999) that attempt to provide a framework for Risk Management within an ISEC context. The GAO Report on ISEC Assessment (1999) defines risk management as consisting of four stages:

1. Risk Assessment
2. Implementing policies
3. Promoting Awareness
4. Monitoring and Evaluation

Thus risk assessment is one element of a broader set of risk management activities. Although each element of the risk management cycle is important, risk assessment provides the foundation for other elements of the cycle. In particular, risk assessment provides a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Risk assessments, whether they pertain to information security or other types of risks, are a means of providing decision makers with the information needed to understand factors that can negatively influence operations and outcomes, and make informed judgments concerning the extent of actions needed to reduce risk. All risk assessments generally include the following elements:

- Identifying threats that could harm, and thus, adversely affect critical operations and assets.

- Estimating the likelihood that such threats will materialize based on historical information and/or the judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected.
- Estimating the potential losses or damages including recovery costs.
- Identifying cost-effective actions to mitigate risk, which includes ISEC policies as well as technical and physical controls. (GAO Report 1999)

Generally two approaches are followed in risk assessment: a quantitative approach and a qualitative approach. A quantitative approach estimates the monetary costs of risk and risk reduction techniques based on the likelihood that a damaging event will occur, the costs of potential losses, and the costs of mitigating actions that could be taken. When reliable data on likelihood and cost are not available, a qualitative approach can be taken by defining risk in more subjective terms. It is also possible to use a combination of quantitative and qualitative methods. Challenges associated with assessing information security risks include:

1. Data are limited on risk factors, such as the likelihood of a sophisticated hacker attack and the costs of damages, loss, or disruption caused by events that exploit security weaknesses.
2. Some costs such as loss of consumer confidence are difficult to measure
3. Although the costs of the hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented.

4. Even if precise information is available, it would soon be out of date due to fast paced changes in technology and factors such as improvements in tools available to would-be intruders (GAO 1999).

So what are the current tools used by the industry for risk assessment? Are they serving the purpose and how grounded are each of the tools in theory? The GAO report (1999) looks at current practices in the industry and reports on the risk assessment tools used by companies known for the superior information security programs. Most of the tools are relatively simple aids to assessment and reporting:

1. Risk assessment matrix: this shows the combined effect of the probability of an undesired event occurring and the severity of damage or loss to key organizational assets or operations if the events were to occur. Different scenarios of information security breaches are developed and are then ranked according to severity level and probability of occurrence. Possible severity levels could be level 1, 2, 3 etc and levels of probability could be frequent, probable, occasional, remote and improbable. Based on these levels and the companies policies risk indexes are assigned to each scenario using a risk assessment matrix. Now a corrective action can be chosen based on 1) the effectiveness of the control in reducing either probability or severity of potential scenario and 2) cost.
2. Questionnaire: this approach uses a questionnaire to document compliance or non-compliance with company control objectives and the specific control techniques employed. The questionnaire is organized by specific control objectives, such as authentication, access control, confidentiality, availability, audit, and administration.
3. Another approach is to use a combination of risk assessment matrix and questionnaire. Essentially the risk assessment matrix is formed using outputs from a questionnaire.

4. Expert systems: to analyze data and to develop recommendations. The system has two main phases:
    a) Data gathering phase: primary activities include determining controls in place and identifying business concerns and potential loss
    b) Analysis phase: primary activities include identifying deviations between current controls and established control objectives, determining the adequacy of the current controls, determining recommendations for additional controls, quantifying any gaps between current controls and desired policy and creating security applications (GAO 1999).

The data gathering procedure involves using a questionnaire to compile information on the value of critical operations and assets, policies and controls in place, and other system attributes. The data analysis as done by the expert system compares this information with predetermined policy and control requirements. The analysis group inputs the information about the current controls, as derived from the questionnaire answers, into a software program. The software program compares these controls to control requirements documented in the company's information security policies. The database of information security control requirements represents a consensus of the experience and best judgment of a broad group of business and information technology experts organization-wide. The analysis performed by the software identifies instances where existing controls do not meet the company's suggested control requirements. Using the result of this comparison, additional information from the questionnaire, and a defined list of control techniques, the expert system automatically proposes control techniques to achieve compliance with control requirements (GAO 1999).

As can be seen from this review of current practices in risk assessment, most of the tools with perhaps the exception of the expert system are primitive and not grounded in theory. There is thus a need to develop a new methodology for ISEC risk assessment, which uses concepts from the literature of risk management. One tool in particular, VAR, is attractive for use in ISEC. VAR can provide a risk estimate for stock portfolios. The question is can it be applied to a 'portfolio of security initiatives'? Markowitz's stock portfolio theory shows us that by diversifying investments in stocks, we can decrease the risk (Finne 1998). Is the same true for an ISEC portfolio? Can we diversify the risks connected to ISEC? In order to answer these questions, risks will have to be operationalized. We will adopt VAR to measure these risks. Once the risks are measured, choosing the optimal security is a standard cost-benefit analysis.

VAR is an estimate of maximum potential loss to be expected, over a given period, over a certain percentage of time. It has gained rapid acceptance as a valuable approach to risk management in the financial arena (Beder 1995). VAR has been used for a long time to measure the risk of an entire portfolio in a single number. It expresses in dollar terms, the major concern of risk management – the potential loss to portfolio value. VAR has primarily been applied to market risk, though applications have recently been expanded to incorporate corporate risk. VAR holds promise of combining all quantifiable risks across the business lines of an institution, yielding one firm-wide measure of risk (Simons 1996).

III. VAR Framework

VAR summarizes the worst possible loss due to a security breach over a target horizon with a given level of confidence. More formally, VAR describes the quantile of the projected distribution of losses over a given period. To illustrate the analytical capability of VAR, it could

provide answers to questions such as how much could a company with $100 million worth of assets lose, due to a security breach over a period say one month?

In order to explain the VAR framework we consider the case of a fictitious company: Retail.com. Retail.com is an online retailer that sells everything from books to CDs. Its net present value is estimated at $100 million. Retail.com has been in business for the last 5 years, and has always been subject to security breaches ranging from hackers to viruses. Last year during the holiday season it was subject to a denial of service attack. As a result of this denial of service attack, the company's web servers crashed resulting in losses worth millions of dollars in terms of lost sales and loss of reputation. The company already had a security policy in place and had invested millions in security initiatives. However it was evident that these measures were not satisfactory and the company needed to reassess its information security risk. The Information Security Manager decided to use the VAR framework for Risk Assessment to evaluate its security preparedness.

The VAR framework for Information Security Risk assessment appears below:

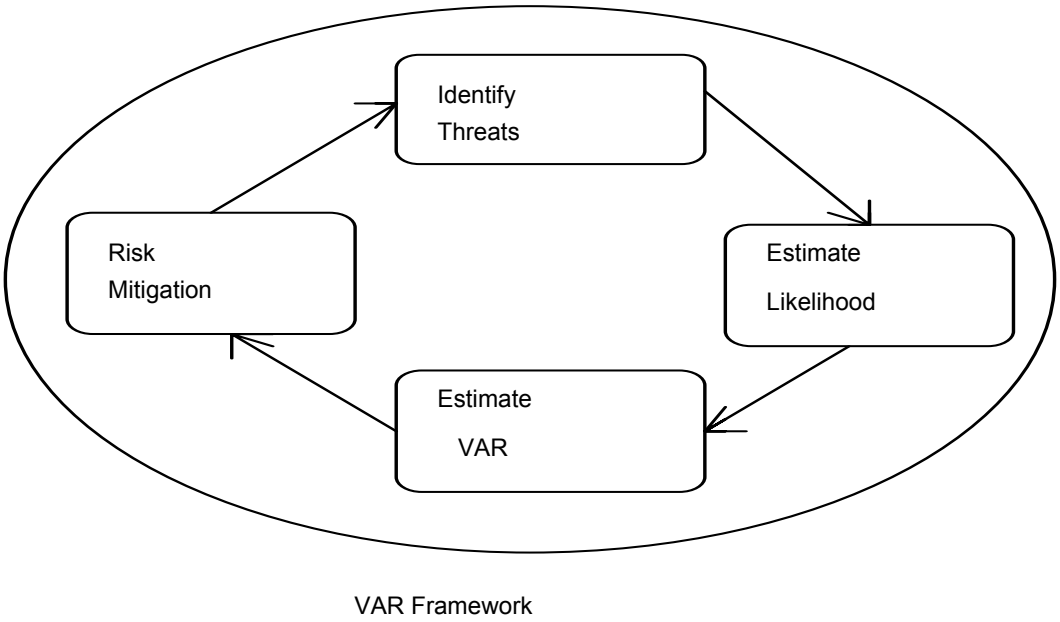

Figure 1: VAR Framework for Information Security Risk Assessment.

The VAR framework for Information Security Risk Assessment consists of four stages: 1. Identifying Threats, 2. Estimating Likelihood of these threats, 3. Calculating Value at Risk and 4. Risk Mitigation. These stages are described in detail below:

1. Threat Identification: The first stage of risk assessment is identifying the threats or potential risks faced by a firm. The GAO report (1998) classifies threats as Frauds, Malicious Acts, Pranks, Attempts to access private information, Natural Disasters, Sabotage and User Error. Microsoft's white paper on security uses a different classification that appears below.

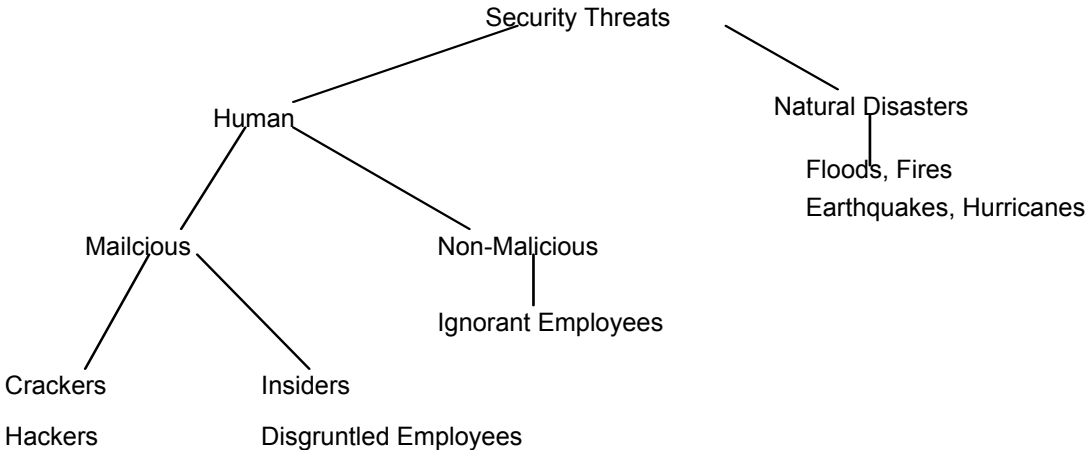

Figure 2: Security Threat Classification (Microsoft Whitepaper on Security 2000)

The motives/goals/objectives could include Denial of Service, Deleting and Altering Information, Information Theft and Disrupting Normal Business Operation. Methods employed exploit the vulnerability within an organization and include viruses, Trojan horses, worms, password cracking, E-mail Hacking, Packet Replay and Network Spoofing. Every organization may be at risk from some or all of these potential types of risks. Thus the first task is to identify the types of risks that each company faces, which would depend on the industry the organization belongs to, the assets, and the type of customers among other things. Retail.com can perform a formal threat identification by conducting a survey of information security managers within or outside the firm or by employing consultants in the industry.

2. Likelihood Estimation: There are a number of surveys, which have reported the frequency of a security breach (Briney 1999, Ernst and Young 1999, Power 1999, Briney 2000). Briney (2000) found that the percentages of respondents experiencing major types of security breaches are viruses (80%), employee abuse (58%), unauthorized access by outsiders (42%) and theft/destruction of data (24%). While such industry figures are useful to the organization, ultimately it will have to decide for itself the likelihood of the risks it might face, especially given the understanding that most security breaches go unreported, especially in particular industries. Estimates of the frequency of unauthorized external access to an organization's systems can be obtained from the access logs. Other estimates of likelihood of threats can be obtained from historical data. Information Security officers within a firm are ideal candidates who can be interviewed to obtain threat likelihood figures. Based on industry survey, log data, historical data and interviews with key security personnel it would be possible for Retail.com to estimate the probability of a distribution of threats. Possible risk scenarios can then be developed based on the probability distributions of individual risks. If the firm faces n risks then there are 2^n possible risk scenarios. With good judgment some of the possible risk scenarios can be eliminated.

3. Estimate VAR: Now that the different risks have been identified, the likelihood of these risks (the probability distribution of risks) estimated and the possible risk scenarios developed, the next step is to calculate the Value at Risk of the firm. Information security managers at Retail.com decided to estimate the VAR over a period of one month at the 99^{th} percentile confidence level, i.e. the maximum amount in dollar terms that Retail.com can lose over a period of one month as a result of security breach 99% of the time. The following steps are required to compute VAR:

- Set Current Market value of company = $100 million
- Calculate variability of risk factors as estimated from distribution of different risk scenarios. Assuming the simplistic case where all the risks are independent, the variability in the risk scenario is the product of the individual probability distributions.
- Set a Time Horizon of 1 month
- Set the confidence level to 99^{th} percentile
- Report the worst-case loss to Retail.com in each case of the risk scenario for the given time horizon. A probability distribution for the worst-case loss can be estimated from this.
- From the estimated probability distribution for worst-case loss, calculate the worst loss for the given confidence level. This value of the loss is the VAR.

Thus VAR summarizes the expected maximum loss (or worst loss) over a target horizon within a given confidence interval. For example, if the VAR in this case was calculated as $10 million, the worst loss would be less than $10 million 99% of the time over a period of one month. The VAR computation can be further simplified if the worst-case loss distribution can be said to belong to a parametric family, such as the normal distribution

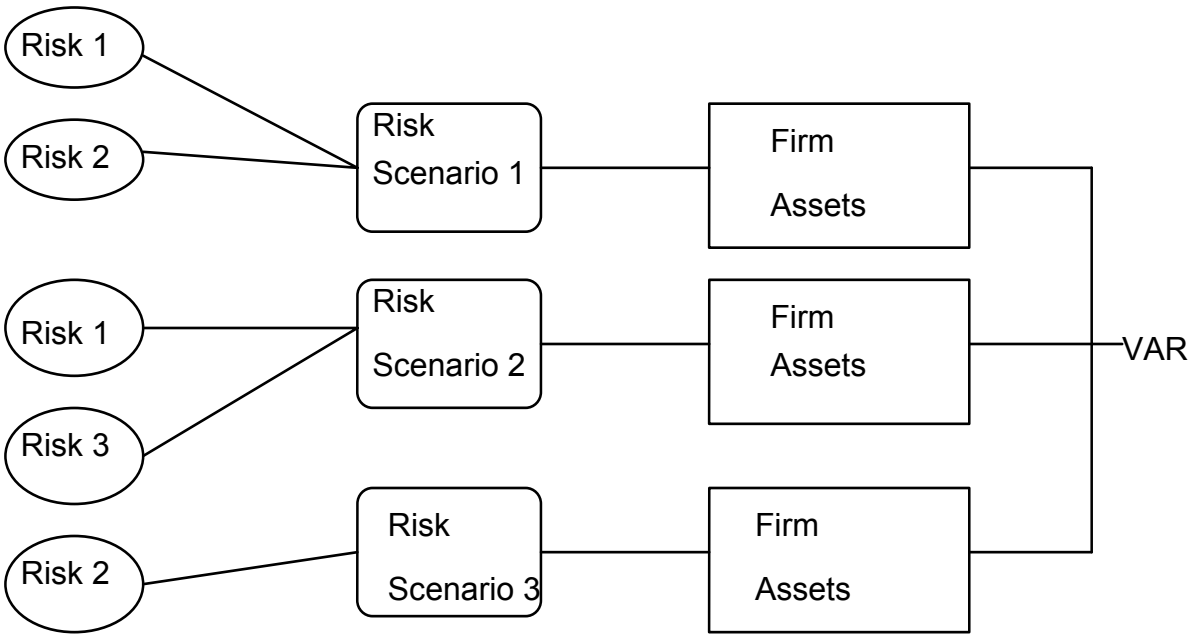

Figure 3: Estimating VAR

4. *Risk Mitigation:* After VAR for Retail.com has been calculated applying the procedure specified above, the next step would be to choose security measures for risk mitigation. A company, which has a smaller VAR, would have to make a smaller investment on security measures than a company that has a larger VAR. The process of calculating the VAR for Retail.com is then repeated assuming that the new security measures are in place. The threats to Retail.com and their corresponding likelihoods are also going to change with the new security measures and this would affect the VAR calculations. After various iterations the right tradeoff between an acceptable VAR and cost of providing security can be achieved.

IV. Conclusions, Limitations and Future Research

Most of the tools that are used for ISEC risk assessment are qualitative in nature and are not grounded in theory. VAR is a well-accepted concept for managing portfolio risk and is well grounded in theory. VAR is a useful tool in the hands of an ISEC expert as it provides a

quantitative measure of information security risk. Using this measure of risk, the right balance between risk and cost of providing security can be achieved. Each firm will have a figure in mind regarding how much risk is acceptable. When the total VAR of a company exceeds this figure, the firm will know that it is time to invest in more security.

The VAR framework presented here although appealing, has its disadvantages. VAR calculation depends on identifying threats and estimating their likelihood. There could be a lot of subjectivity involved in the VAR calculation when the estimates are based on the knowledge of individual security personnel rather than on security surveys and historical data. Additionally, security surveys can only provide an estimate of the likelihood of threats across an industry, rather than for an individual firm. An individual organization's risk scenario might be very different. VAR can only provide a worst-case loss rather than an average loss value. A simplistic example of a fictitious company Retail.com is presented here to demonstrate the VAR framework. Extensive testing of the VAR framework on real company data is needed.

References:

Beder, T.S. (1995) VAR: Seductive but Dangerous, *Financial Analysts Journal*, 51 (5), pp.12-25.

Bequai, A. (2000) America's Internet Commerce and The Threat of Fraud, *Computers and Security*, 19 (8), pp. 688-691.

Bhimani, A. (1996) Securing the Commercial Internet, *Communications of the ACM,* 39 (6), pp. 29-35.

Briney, A. (1999) Got Security? *Information Security*, available at http://www.infosecuritymag.com/articles/1999/julycover.shtml.

Briney, A. (2000) Security Focused, *Information Security* available at http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf

Caelli, W., Longley, D. and M. Shain (1989) *Information Security for Managers*, Stockton Press.

Ernst and Young (1999) 6th Annual Information Security Survey,

http://www.ey.com/global/vault.nsf/US/6th_Annual_Information_Security_Survey/$file/FF0156.pdf

Finne, T. (1998) Information Security Implemented in: the Theory on Stock Market Efficiency, Markowitz Portfolio Theory and Porter's Value Chain, *Computers and Security*, 17 (4), pp. 303-307.

Finne, T. (1997) A Conceptual Framework for Information Security Management, *Computers and Security*, 16 (6), pp. 469-479.

GAO Report (1999) Information Security Risk Assessment – Practices of Leading Organizations, Report No. AIMD-99-139.

GAO Report (1998) Information Security Management – Learning from Leading Organizations, Report No. AIMD-98-68.

Microsoft Whitepaper on Security (2000) available at http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/bestprac/secthret.asp

PFIRES (2000) *Policy Framework for Interpreting Risk in eCommerce Security,* Accenture and CERIAS, Purdue University.

Power, R. (1999) 1999 CSI/FBI Computer Crime and Security Survey, *Computer Security Institute*, 5 (1).

Oppliger, R. (1997) Internet Security: Firewalls and Beyond; *Communications of the ACM,* 40 (5), pp. 92-103.

Sherwood, J. (2000) Opening up the Enterprise, *Computers and Security,* 19 (8), pp. 710-719.

Simons, K. (1996) Value at risk – New approaches to risk management; *New England Economic Review*, Sept/Oct, pp. 3-14.

Turban, E, J. Wetherbe and E. McLean (1996) *Information Technology for Management: Improving Quality and Productivity*, John Wiley and Sons.