Computers & Security (2005) **24**, 16–30

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Management of risk in the information age

Mariana Gerber[1], **Rossouw von Solms***

Department of Information Technology, Port Elizabeth Technikon, Private Bag X6011, Port Elizabeth 6000, South Africa

Received 26 October 2004; revised 23 November 2004; accepted 23 November 2004
Available online 28 January 2005

KEYWORDS
Information security;
Information security management;
Risk analysis;
Information security requirements

Abstract Linked together, organisations can exchange information and engage in transactions in ways unanticipated before, the emphasis being on information, which became core to most business activities and without which business will fail to operate [Owens S. Information security management :an introduction. London: British Standards Institution; 1998. pp. 1–2]. Consequently, to contribute to ensuring business continuity, the protection of information resources had to be pursued. Risk analysis was traditionally used to analyse risks posing a threat to mostly IT assets [Jung C, Han I, Suh B. Risk analysis for electronic commerce using case-based reasoning. International Journal of Intelligent Systems in Accounting, Finance & Management 1999;8:61–73. John Wiley & Sons, Ltd., p. 62]. Resulting in recommendations for the implementation of appropriate security measures, to reduce those identified high priority risks to an acceptable level. However, Bandyopadhyay et al. [Bandyopadhyay K, Mykytyn PP, Mykytyn K. A framework for integrated risk management in information technology. Management Decision 1999;37(5):437–44. MCB Press, p. 440] state that the evaluation of risk related to IT alone is unrealistic. A holistic view of assessing risks should instead be adopted, moving away from the isolated and partial view of today's ''closed world assumption'' of searching only within a specific domain to evaluate the risks associated to IT, to consider the entire spectrum related to the IT environment. Thus an alternative approach to risk analysis might have to be developed, to assist in analysing risks to information-specific resources.

* Corresponding author. Tel.: +27 41 504 3604; fax: +27 41 504 9604.
E-mail addresses: mariana@petech.ac.za (M. Gerber), rossouw@petech.ac.za (R. von Solms).
[1] Tel.: +27 41 504 3705; fax: +27 41 504 3313.

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.11.002

Introduction

Risk analysis is essentially used to identify, estimate and evaluate risks (Frosdick, 1997, p. 165). Jung et al. (1999, p. 62) give a more elaborate definition of risk analysis and define it as "a systematic process to examine the threats facing the IT (information technology) assets and the vulnerabilities of these assets and to show the likelihood that these threats will be realised". Thus, risk analysis was conventionally a way in which risks to IT assets could be identified and quantified, to determine the probability of risk occurring and the consequence thereof should an adverse event happen causing that risk to materialise. Risk analysis is thus deemed appropriate for securing computer assets (referred to a IT assets), which are mostly physical of nature and of which the threats and vulnerabilities can be estimated by means of qualitative and/or quantitative measures (Humphreys et al., 1998, p. 49). Consequent to the risk analysis, the evaluated risks have to be properly managed. Risk management involves high priority risks to be reduced to an acceptable level by applying appropriate security measures.

With the onset of the information age, information became a vital resource — "the lifeblood of a business" as stated by Wills (1999, p. 1), Minister for Small Firms, Department of Trade and Industry. Information has extreme value to an organisation (BS 7799-1, 1999, p. 1; Humphreys et al., 1998, p. 8) and just like any other valuable asset information has to be adequately protected (URN 99/704, 1999, p. 1), to ensure business continuity. Wills (1991, p. 1) further articulates that nowadays it is not just about protecting the technology, but also to a large extent about protecting business or personal information wherever it resides. The emphasis has thus moved more towards the protection of information than merely the infrastructure, which arguably used to be the focus of traditional risk analysis.

Although asset valuation is a vital part of risk analysis, quantifying information could prove to be a rather daunting task. The quantification of risks to physical or tangible assets already proved to be an extremely difficult task, how much more not so for estimating the risks to information. This is supported by an observation made by Burch et al. (1979, p. 16) stating that with information, which is an example of an intangible asset, it is extremely difficult if not impossible to determine precise value. This gives way to the following question: "Could it be possible that the information society has outgrown the approach that traditional risk analysis utilises?

The objective of this paper is twofold. Firstly, to motivate why the methodology utilised by traditional risk analysis might not be adequate for ensuring the proper protection of information. Secondly, to investigate the factors that an alternative approach to traditional risk analysis should typically include in order to holistically manage risks, not only to tangible assets, but also intangible assets alike.

The discussion will start with defining the term risk and where it originated from, moving to an interpretation of risk in IT. Motivation for adopting an alternative approach to traditional risk analysis will follow and the paper will end with suggestions on factors to consider in establishing the unique information security requirements of an organisation.

Evolution in the meaning of risk in general

The concept of risk is a complex one, causing a lot of ambiguity between natural and social scientists. The meaning of risk has evolved over time and its development has been outlined by Douglas (1990) starting from the seventeenth century to date.

The concept of risk originated in the seventeenth century with the mathematics associated with gambling. Risk referred to a combination between probability and magnitude of potential gains and losses. During the eighteenth century risk, seen as a neutral concept, still considered both gains and losses and was employed in the marine insurance business. Risk in the study of economics emerged in the nineteenth century. The concept of risk, by now, seen more negatively, caused entrepreneurs to call for special incentives to take the risk involved in investment. By the twentieth century a total negative connotation was made when referring to outcomes of risk in engineering and science, with particular reference to the hazards posed by modern technological developments such as in the petro-chemical and nuclear industries.

Definition of risk (natural sciences vs. social sciences)

Definitions of risk in general as described by Royal Society (1983, 1992) started with "the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge" (Royal Society, 1992, p. 2). To support Royal Society Study Group's acknowledgement for

the need of engineers and scientist who specialize in risk studies, the 1992 report included definitions of risk, based on the British Standard 4778, as ''a combination of the probability or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence'' (British Standards Institution, 1991).

Since there is a difference in perception of individual and societal risks, it is important that distinction be made between these kinds of risk. An individual risk has been defined by the Health and Safety Executive as ''the risk to any particular individual, either a worker or a member of the public, [that is] anybody living at a defined radius from an establishment, or somebody following a particular pattern of life'' (HSE, 1988, para. 52). A societal risk (synonymous for societal: communal, community, common, public, shared, collective, and group), on the other hand, represents the risk to society and is defined as ''measured, for example, by the chance of a large accident causing a defined number of deaths''. According to Warner (1993) these definitions of risk forms the foundation from which scientists and engineers conduct practical work. It mainly involves putting numbers on risk, based firstly on calculations of probabilities and secondly, on the use of databank information on failures and reliability, to determine consequences in terms of fatalities. In order to gain a better understanding of terms such as *scientist* and *science* and its relevancy to risk, it will be necessary to discuss the various sciences in more detail.

When investigating the classification of the different sciences, it becomes clear that three paradigms can be distinguished, namely the natural sciences paradigm, the theoretical or abstract sciences paradigm and the social sciences paradigm, as illustrated in Fig. 1.

Natural science is defined by the Oxford dictionary as ''the sciences used in the study of the physical world'' (Oxford advanced learner's dictionary, 1995) which ''deals with the objects, phenomena, or laws of nature and the physical world'' (The American Heritage® dictionary of the English language, 2000). Merriam-Webster's collegiate dictionary (2002) defines it as ''any of the sciences (such as physics, chemistry or biology) that deal with matter, energy and their interrelations and transformations or with objectively measurable phenomena''. Another definition of natural science is that it ''attempts to explain the natural universe'' or that it ''involves a process by which to investigate the natural universe'' (Krupp, 1999). It should be noted that according to Original Roget's® thesaurus of English words and phrases (1992), the English term *science*, is usually considered to be a synonym for *natural science* (Suojanen, 2000, p. 14).

The natural science paradigm groups together various other science disciplines, as shown in Fig. 2. It encompasses science disciplines such as physical science, life science and applied science (Original Roget's® thesaurus of English words and phrases, 1992). Life science includes those subjects involving the study of plants, animals, etc. such as biology, botany whereas physical science is concerned with the study of inanimate or non-living natural objects (Oxford advanced learner's dictionary, 1995). Examples of subjects, which can be classified under physical science, are physics, chemistry, astronomy and meteorology.

Applied science is the art or science of making practical application of the knowledge of pure sciences, such as physics or chemistry, to practical problems (Infoplease.com, 1998–2004; WordNet® 1.6, 1997). An example of an applied science is the engineering discipline shown in Fig. 2. Engineering is the practical application of either, science or scientific or mathematical principles derived from

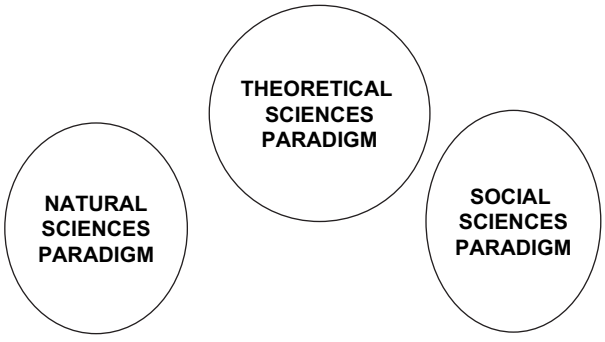

Figure 1 The paradigms of the theoretical sciences, natural sciences and the social sciences.

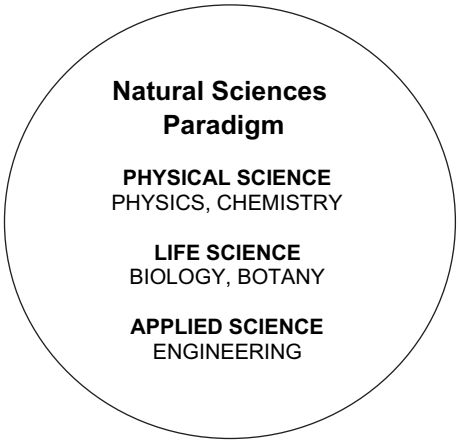

Figure 2 Grouping of science disciplines within the natural science paradigm.

knowledge of the mathematical and natural sciences (Stark, 2003), to meet practical ends in industry or commerce. Practical applications include the design, manufacture, building, operation and control of economical structures, machines, processes, systems, roads, bridges, electrical apparatus or chemicals (Oxford advanced learner's dictionary, 1995; WordNet® 1.6, 1997; The American Heritage® dictionary of the English language, 2000).

Synonyms for *engineering* include words like *mechanics, production* and *technology*. (Original Roget's® thesaurus of English words and phrases, 1992). Electrical engineering is but one of the various fields into which the engineering discipline can be divided. As depicted in Fig. 3, computer engineering is in turn regarded as one of the branches of electrical engineering (Stark, 2003).

Computer engineering, almost unknown just a few decades ago, is now classified as one of the most rapidly growing fields. Microminiaturization is one of the current trends in computer engineering and strives to continuously increase the number of circuit elements that can fit onto smaller chips. Other trends are the use of parallel processors and superconducting materials (Stark, 2003) to increase computing speed. However, the creation of sophisticated programs to promote "artificial intelligence" and the development of higher level machine languages are deemed to be closer related to computer science than to computer engineering (Weems, 2003).

Computer science is a combination between theory, engineering and experimentation. It provides a platform for the design and use of computers. Based on the knowledge that computer science originated from mathematics and engineering (Weems, 2003), computer science is believed to be positioned on common ground between the natural science paradigm and the theoretical (abstract) science paradigm as depicted in Fig. 4.

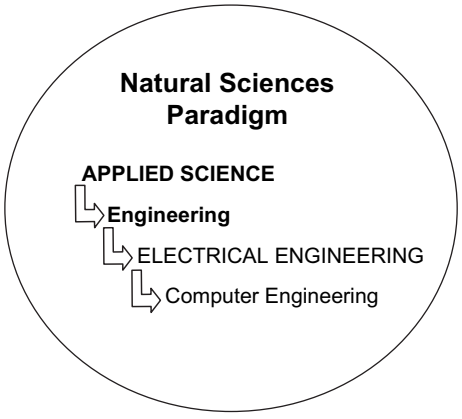

Figure 3 Hierarchy within the natural science paradigm.

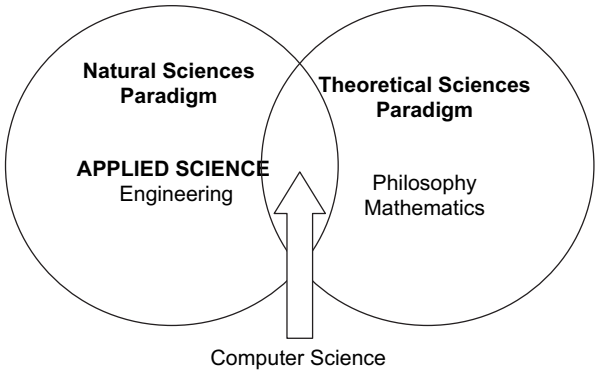

Figure 4 Positioning of computer science discipline within the natural science paradigm and the theoretical science paradigm.

Its approaches are therefore regarded as being highly mathematical and logical. It was not until the introduction of the first electronic digital computers in 1940 that computer science was recognised as being different from mathematics and engineering (Weems, 2003). Despite their differences, the fields of computer science and computer engineering (a branch of engineering) are closely related (Stark, 2003) within the natural sciences paradigm, as shown in Fig. 5.

Note that all further reference of the natural science paradigm within this document implies the inclusion of mathematics from the theoretical science paradigm. Due firstly, to computer science having roots in both of these paradigms and secondly, due to mathematics providing many core methods for the natural sciences (Wikipedia, 2004). Natural science or "science", as it is alternatively referred to, develops using a systematic approach, known as scientific method, based on objective analysis rather than personal belief (Burnie, 2003). This characteristic of natural science, distinguishes natural science from social science.

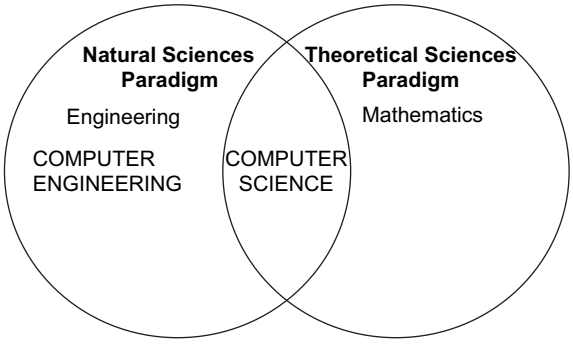

Figure 5 The computer science discipline in relation to the computer engineering discipline.

Within the social science paradigm, social science is defined as the study of society and social behaviour or a science or field of study dealing with an aspect of society or forms of social activity (Infoplease.com, 1998–2004; Oxford advanced learner's dictionary, 1995). The U.S. Department of Labor (2002–2003) specifies that it is a study involving all aspects of society – covering past events and achievements as well as human behaviour and relationships between groups. Social science consists of a number of disciplines. It includes disciplines such as economics, politics, government, legislation, law, criminal justice, anthropology, culture, ethics, religion, history, geography, psychology, sociology and gerontology, as illustrated in Fig. 6 (University of Maryland University College, 1996–2003; Central Oregon Community College, 2003; Miami-Dade Community College, 2003; U.S. Department of Labor, 2002–2003; Glenn, 1989–2001).

It can be argued that the most obvious difference between the natural sciences and the social sciences is that, the natural sciences deal more with objectively measurable phenomena, whereas the social sciences are more involved with human behaviour and social activity.

The question that now arises is "How does the concept of risk and the evaluation thereof relate to the two defined paradigms?" Various techniques for evaluating risk exist. These techniques stem from the different approaches of engineering, economics, behavioural sciences and politics. The engineering field, which relates to the natural science paradigm (refer to Fig. 2), has described risk assessment as being "a field of objective, scientific analysis (Mayo and Hollander, 1991). Frosdick (1997, p. 172) goes further by stating, "the engineering paradigm is one of quantification" and focuses more on technology than on people since its techniques employ quantified comparisons and is technically inclined.

Figure 6 Grouping of science disciplines within the social science paradigm.

On the other hand social scientists provide information that helps us understand the different ways in which individuals interact, make decisions, exercise power and respond to change (Miami-Dade Community College, 2003; U.S. Department of Labor, 2002–2003). Thus, the way in which social scientists evaluate risk is by subjective public perception based on values, belief and opinion, which are influenced by factors such as history, culture, politics, law and religion. Kirkwood describes a subjective or perceived risk as one arrived at without a scientific assessment (Kirkwood, 1994, p. 15).

It is clear at this stage that the concept of risk in the natural sciences paradigm is seen as an objective or evaluated risk, due to the scientific assessment methods used to evaluate risk. An objective risk evaluation is non-judgemental (Kirkwood, 1994, p. 17) and follows precise calculations, formulae and exact experiments. Within the social science paradigm, however, risk is seen as subjective or perceived risk, since it is a decision, which is arrived at without a scientific assessment. The subjective risk evaluation is based on perception, heuristics or rule-of-thumb guidelines. Rule-of-thumb being a decision arrived at by utilising experience, judgement and ingenuity (Kirkwood, 1994, p. 19) rather than pure mathematics. From this it can be seen that there is a distinct difference in the way that risks are assessed in the natural science paradigm versus that of the social science paradigm. With this distinction in mind and in order to investigate the concept of risk further, an explanation on how risk is defined within the computer science branch of information technology will follow.

Definition of risk in IT

Science has a profound effect on the way we live, largely through technology. Technology, being the use of scientific knowledge for practical purposes (Burnie, 2003). Although both the fields of engineering and information technology are known to be synonymous with technology, information technology also has strong ties to computer science. Thus, information technology is depicted between engineering and computer science within the illustration shown in Fig. 7.

Since both the disciplines of engineering and information technology are synonymous with the

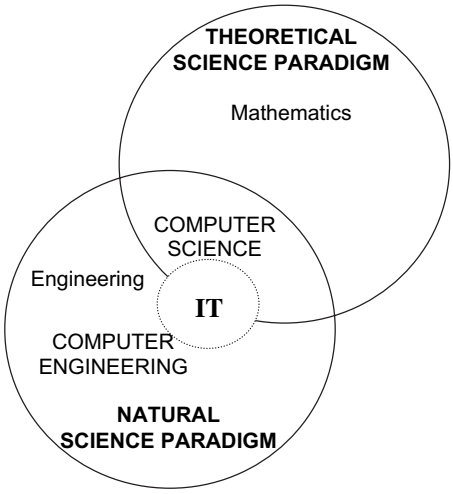

Figure 7 Positioning the field of information technology.

term *technology* it seems appropriate to consider the 1995 publication of National Institute of Standards and Technology (NIST) handbook's definition of risk which describes risk as ''the possibility of something adverse happening'' (NIST, 1995, p. 59). The 2001 publication of NIST handbook defines risk as ''the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence'' (NIST, 2001, p. 1). Another appropriate definition of risk, related to the computing environment in particular, as stated by Kailay and Jarratt (1995) is ''the potential for damage to a system or associated assets that exists as the result of a combination of a security threat and a vulnerability. The risk exists because of the combination of threats, vulnerability and asset value. A vulnerability being a weakness in the security system that might be exploited to cause loss of or harm to the asset(s) (Pfleeger, 1989) and a threat being the source or circumstance that has the potential to cause loss or harm (Kailay and Jarratt, 1995; Pfleeger, 1989).

A lot have been said regarding the concept of risk, however, Douglas (1992, p. 15) states ''political pressure is not explicitly against taking risks, but against exposing others to risk''. The primary function of modern civil law is therefore to control risk (Priest, 1990), which emphasises the link with accountability. The link with accountability is elaborated on by Priest who specifies that ''a party to an injury will be held liable by court if that party could have taken some action to reduce the risk of the injury at a cost less than the benefit from risk reduction''. As for any risk, regardless of whether resulting in injury to an individual or society or whether causing damage to a system or to any other asset, it needs to be reduced. In order to reduce risk it has to be managed in some way. There does, however, exist some confusion regarding the true meaning of the expression ''risk management''. The next section will put into perspective what exactly is meant when referring to ''risk management'' and what is meant when referring to ''management of risk''.

Management of risk

Risk management ''refers to planning, monitoring and controlling activities which are based on information produced by risk analysis activity'', whereas the management of risk is described as the ''overall process by which risks are analysed and managed'' (Scarff et al., 1993, p. 2), as illustrated in Fig. 8.

According to the previous explanation it can be concluded that risk management should be preceded by some risk analysis activity (Bandyopadhyay et al., 1999, p. 443; Owens, 1998, pp. 8–9; BS 7799-2, 1999, p. 2; Moses, 1992, pp. 229–230). Together, the process of risk analysis followed by the process of risk management can be considered part of the overall management of risk. Both these processes, risk analysis and risk management, will individually be discussed in more detail.

Risk analysis

All further reference of the term risk analysis, within this article/paper will use a definition as proposed by Frosdick (1997, p. 165). This definition suggests that risk analysis is the sum of risk identification, estimation and evaluation (see Fig. 9).

The basic stage of risk analysis, as illustrated in Fig. 9, is risk identification (Tchankova, 2002, p. 290). As its name indicates, its primary purpose is to identify risk and as explained earlier, risk comprises a combination of asset, threat and

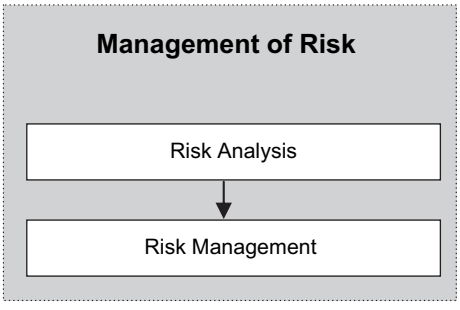

Figure 8 The processes within the overall management of risk.

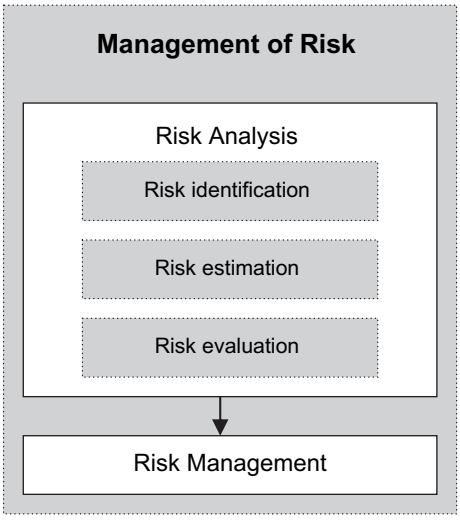

Figure 9 The sub-processes of risk analysis.

vulnerability (ISO/IEC TR 13335-1, 1996, pp. 5–10). It is therefore necessary to identify IT assets (within an established boundary), identify threats to assets and note vulnerabilities (Jung et al., 1999, p. 62).

Once the risks have been identified, *risk estimation* follows. Risk estimation is nothing but putting values on risk. Monetary values being assigned should preferably be related to the cost of obtaining and maintaining the asset (Humphreys et al., 1998, p. 22). Identified risks are usually quantified as a two-dimensional approach, taking into account both the probability of the risk occurring and its consequences should it occur. The quantification of fault and event trees can assist in calculating the probability of various events occurring, whereas the quantification of consequence can be achieved by using a combination of either computer modelling techniques, testing or expert value judgements (Frosdick, 1997, p. 170).

Once risks have been quantified, by estimating both the probability of its occurrence and the magnitude of its consequence, it can be assessed to indicate the tolerability or acceptability of the risk. Hence the term, risk assessment, which was formerly often mistaken as a substitute for risk analysis, but is in fact the third stage of risk analysis. Although certain sources refer to risk assessment and others to risk evaluation, the activity that takes place during this stage of risk analysis is conceptually the same. Therefore, from this point onwards, the term *risk evaluation* will be used to describe the assessment of risk. Risk evaluation is nothing but calculating the risk based on the values assigned during risk estimation, for probability and magnitude (impact or severity of harm).

As mentioned earlier, scientists and technologists follow a precise methodology when evaluating risk. This process of risk evaluation is often referred to as ''Probalistic Risk Assessment'' which is a three-stage process. Firstly to determine what can go wrong, secondly to determine the probability of it going wrong and thirdly to determine how severe the consequences would be if it did go wrong. Kirkwood (1994, p. 17) highlights the evaluation of risk as:

$$\text{Risk} = \text{probability} \times \text{severity of harm}$$

The evaluation of risk in this way places a negative connotation on risk and portrays that risk is bad. Although strange at first, risk is, however, still a neutral concept, as it used to be viewed during the seventeenth and eighteenth century (Douglas, 1990). It is equally correct to see risk as something going right, as something going wrong.

A more refined version by Kirkwood based on risk as a neutral concept is:

$$R = P(D - B)$$

where R = risk, P = probability, D = damaging effects, and B = beneficial effects.

The subtraction of beneficial effects from damaging effects (D–B) in producing the severity of harm thus links onto the initial view of risk during the seventeenth and eighteenth century where both gains and losses associated to risk were considered. (Douglas, 1990). In doing so a clearer reflection of the actual severity of harm can be produced.

The estimation of risk, including its probability of occurrence and severity of harm, requires deep knowledge, since it is classified as experience intensive and requires domain experience (Jung et al., 1999, p. 61). Even with the availability of experienced risk analysts, risk analysis often relies on nothing more than mere guesses (Pfleeger, 1997, p. 470). The guessing involved in both quantitative and qualitative risk analysis techniques therefore contributed to a large extent to the subjective nature of risk analysis, as noted and commented on by many researchers (Bandyopadhyay et al., 1999, p. 443; Fung et al., 2003, p. 1; Pfleeger, 1997, p. 471; Lichtenstein, 1996, p. 21; Kirkwood, 1994, p. 17; Jacobson, 1996, p. 1). The risk arrived at, according to Kirkwood (1994, p. 15) as the result of a scientific assessment is referred to as objective or evaluated risk, whereas a decision on the existence of risk arrived at without a scientific assessment, as subjective or perceived risk.

Due to risk analysis ensuring that the decision-making processes of risk management are scientifically informed and due to it being synonymous with the identification and valuation of risks to protect mostly physical (tangible) assets, e.g. infrastructure and hardware, it is assumed to fit within the natural science paradigm, as shown in Fig. 10.

This discussion on risk analysis is concluded with a summary by Frosdick (1997, p. 176), who emphasises the importance of risk analysis techniques, by saying that it is the results produced by these techniques that ensure that the decision-making processes of risk management are scientifically informed.

Risk management

Once the process of risk analysis is complete, risk management should follow. As defined earlier, risk management "refers to planning, monitoring and controlling activities which are based on information produced by risk analysis activity" (Scarff et al., 1993, p. 2). It involves the identification and implementation of security controls to reduce risks to an acceptable level as indicated by the assessed measure of risk (Moses, 1992, p. 230). Risk reduction can be achieved by avoiding risk, transferring risk, reducing the likelihood of threats, reducing the vulnerabilities, reducing the possible impacts, detecting unwanted events early, reacting and recovering (Moses, 1992, p. 236). The choice of risk reduction depends on the specific business environment and circumstances in which the organisation conducts its business. Even after all security controls are in place, there will still be some form of risk remaining. The remaining risk is called residual risk. The residual risk might be the result of some assets being intentionally left unprotected either because of low risk being assessed or because of the high cost of the suggested control. Residual risks need to be classified as either being "acceptable" or "unacceptable". Unacceptable risks should not be tolerated and decisions should be taken to apply additional controls or more stringent controls, which will further reduce risk (Humphreys et al., 1998, p. 27).

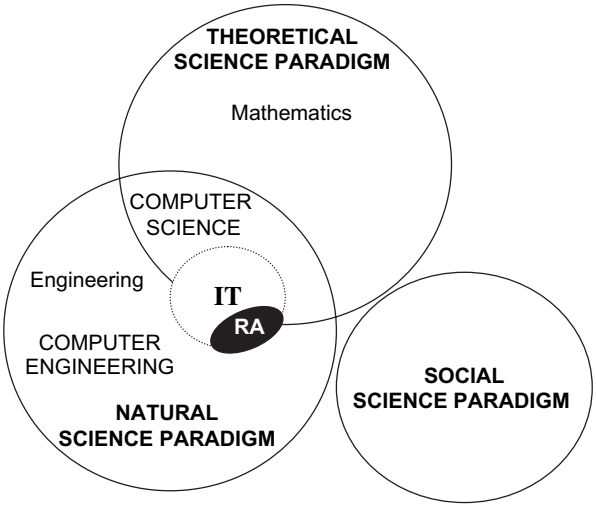

Figure 10 Relating risk analysis to the defined science paradigms.

As explained earlier and as illustrated in Fig. 9, the overall management of risk systematically passes through the processes of identifying, assessing and evaluating risk, collectively termed risk analysis to eventually feed into the process of risk management. The primary function of risk management is to identify appropriate security controls to reduce risks based on the results of the risk analysis, which preceded the risk management process. It should be realised that the management of risk does, however, not end when risk management is complete. It is a continuous process that depends directly on the changes of the internal and external environment of the organisation (Tchankova, 2002, p. 290). It is a fact that change is inevitable. Especially in the IT environment, where rapid advancements in technology took place and is expected to continue advancing at an accelerated pace in future. The effects that these rapid advancements within the IT environment pose on the way in which risk analysis is done will be discussed in the following section.

Management of risk today: "The Winds of Change"

As discussed earlier, the engineering field, which relates to the natural science paradigm, has described risk assessment as being "a field of objective, scientific analysis that can be divorced from political values that forms part of risk management" (Mayo and Hollander, 1991). From this it became evident that the engineering techniques employ quantified comparisons and is technically inclined, which supports the claim by Frosdick (1997, p. 172) that "the engineering paradigm is one of quantification" and focuses more on technology than on people. After all science is believed to develop through objective analysis rather than personal belief (Burnie, 2003).

Unlike scientists and engineers, social scientists do not share this rigid view of risk as a quantifiable and purely technical concept especially when

''a particular risk or hazard [means] different things to different people in different contexts'' and more so if ''risk is socially constructed'' (Royal Society, 1992, p. 7).

Although the engineering discipline focuses more on technology than on people (Frosdick, 1997, p. 172), engineers do, however, acknowledge that ''risk perception depends very much on beliefs, feelings and judgements [and] has major influence on the tolerability or acceptance of risk'' (Strutt, 1993, p. 7). Nevertheless, the techniques used in the discipline of engineering, which form part of the natural science paradigm, is more concerned about the identification of technical failures than it is about social issues, such as risk perception, cultural bias and human communication failures.

Social scientists strongly oppose this view of natural scientists and engineers regarding the management of risk and warns that ignoring sociological/social issues could prove problematic, since the result of human error or lack of communication could be as disastrous as the result of technical failure (Frosdick, 1997, pp. 169 and 176).

The evaluation techniques of risk analysis should thus treat risk as a collective construct, because when it comes to what an acceptable risk is, judgement differs (Frosdick, 1997, p. 175). Judgement varies from subjective perception to physical science, and in the middle is an area of shared beliefs and values (Douglas and Wildavsky, 1982). Dr Michael Hartoonian from Alaska Department of Education & Early Development states that separating tools from culture leads to half-truths and disillusionment (Hartoonian, n.d.).

Applying these views to the overall management of risk shows that risk analysis should not only consider the scientific processes of the natural sciences paradigm. It is strongly advised that, although it contributes to subjectivity, elements from the social sciences paradigm should also be taken into account. Deuchar (2003), CEO of the recruitment company, The Oval Office, says that overlooking the human risk component could cost millions of rand in termination payments, training and placement fees, lost productivity, indirect damage to the company's image and lost opportunities, all because of the human factor often being left out of the risk management equation. Thus, when trying to visualise the management of risk in context of the two defined paradigms, it becomes apparent that the natural science paradigm and the social science paradigm should move closer together, causing an overlap with information being the linking factor (see Fig. 11). This claim is supported by Roth (2003, Section 3), head of Alexander Forbes' Legal Risk Services team, who states ''Information, in all its forms, is arguably one of the most important assets of an organisation. In this context 'information' refers to more than just technology. It refers to the integrity, availability and confidentiality of the lifeblood of the organization, including business trade secrets, contractual relationships, financial and operational systems, client and transaction details and information published to the public''. Clearly showing that both the natural science paradigm and social science paradigm are represented/included when referring to information. Thus, relying on more than just technology, for its protection, but in addition on human involvement/behaviour as well. In the next sub-section it will further be highlighted why information, which can be considered the link that binds the two paradigms, is deemed so important.

Importance of and need for information in the current e-commerce environment

The evolution of the computing environment brought about two major considerations.

Firstly, due to the evolution of the computing environment and the interconnectivity of organisations, information became an integral part of how organisations went about their daily business. The evolution of computing is now, however, at a stage where electronic commerce (EC) seems to have become essential for an organisation's survival and growth (Jung et al., 1999, p. 61). Hence the statement that we live in a society which is mainly driven by information (URN 99/704, 1999, p. 2).

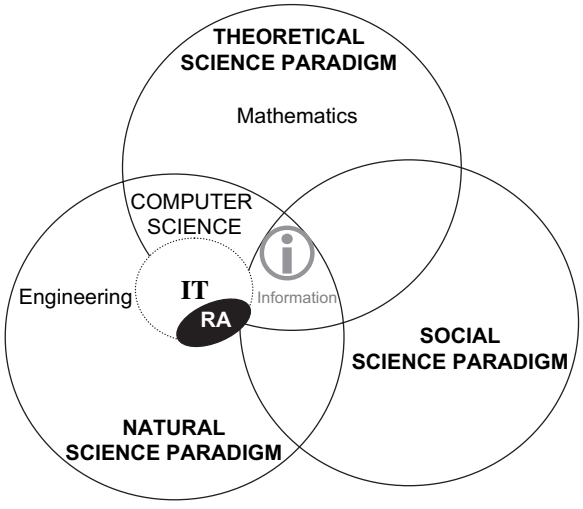

Figure 11 Linking the defined science paradigms.

Just like any other asset, information has to be adequately protected (URN 99/704, 1999, p. 1). As discussed earlier, traditional risk analysis was used to identify, estimate and evaluate risks in order for these risks to be properly managed by reducing these high priority risks to an acceptable level. Reducing the risk by applying appropriate security measures ultimately led to the asset in question being properly secured. The quantification of risks to physical or tangible assets already proved to be an extremely difficult task, how much more not so for estimating the risks to information, which is an intangible asset. Especially in light of the observation made by Burch et al. (1979, p. 16) that with information, which is an example of an intangible asset, it is extremely difficult if not impossible to determine precise value. Frosdick (1997, p. 171) agrees that a risk cannot be treated as a concrete physical entity. Traditional risk analysis is good for securing computer assets, which are mostly physical of nature and of which the threats and vulnerabilities can be estimated by means of qualitative and/or quantitative measures (Humphreys et al., 1998, p. 49).

It thus appears as if the information society of today has outgrown the approach that traditional risk analysis utilises. Especially with information being regarded as a multiplier resource. It has multiplied to such extent that its vastness has by far exceeded one's capacity to absorb even relevant material (Smithson 1991, p. 9), which complicates its protection even further.

Due to information being assumed as a link between both the natural science paradigm and the social science paradigm as explained in Fig. 11, evaluation techniques of both paradigms should be incorporated when attempting to manage risk to information successfully. By considering the natural sciences paradigm on its own or in turn by considering the social science paradigm on its own, to achieve this goal would therefore not be a viable option.

As explained before, the overall management of risk starts with risk analysis, followed by risk management. It is said that the results produced by the risk analysis techniques ensure that the decision-making processes of risk management are scientifically informed (Frosdick, 1997, p. 176). Traditional risk analysis has been and still is synonymous with the identification and evaluation of risk to protect physical assets such as infrastructure and hardware. Due to it making use of scientific methods and since it is focussed on IT infrastructure, it can be argued that traditional IT risk analysis falls within the natural science paradigm. Regardless, risk analysis ends up in risk management, which is mainly the identification of security controls. With risk management, which involves the selection of security controls, in mind it should, however, be noted that nowadays it is more about protecting the information than merely the infrastructure (Wills, 1999, p. 1) as used to be the case with traditional risk analysis. The protection of information needs to be given serious consideration especially in the light of it becoming such integral part of business and of it being assumed the link between the two paradigms of natural science and social science (see Fig. 11).

Since the natural science paradigm has already been considered by means of traditional risk analysis, other alternative approaches in addition to traditional risk analysis might therefore be required to ensure that firstly, the information resources of an organisation is properly secured (Moses, 1992, p. 229) and secondly, the social sciences paradigm is considered in the overall management of risk. After all, if an alternative approach can also lead to the identification of security controls, it could cause the management of risk to be that much more effective.

Secondly, the evolution of the IT environment has also brought about that business processes can no longer be conducted in isolation. Especially in the light of information being regarded as the core to all business transactions and processes. In an e-commerce environment the internal systems and processes of an organisation are no longer operated in isolation from one another (Jung et al., 1999, p. 61). Organisational departments are interrelated and are totally interdependent (Gerber and von Solms, 2001). Linked together, organisations can exchange information and engage in transactions in ways unanticipated before. These interdependencies show that organisations are operating as a whole and since it is recommended that each organisation practice proper information security management (Boddington and Hill, 1998, p. 6), information security should therefore also be considered in a holistic way and no longer partially as is currently the case. This view is supported by Bandyopadhyay et al. (1999, p. 440) who state that the evaluation of risk related to IT alone is unrealistic. A holistic view of assessing risks should instead be adopted, moving away from the isolated and partial view of today's ''closed world assumption'' of searching only within a specific domain, to evaluate the risks associated to IT, to considering the entire spectrum related to the IT environment.

Even more reason why traditional risk analysis might have to be re-focussed or perhaps enhanced

with an alternative approach to properly and holistically secure the information resources of organisations in the current e-commerce environment.

From the literature and from what have been discussed in the previous sections it becomes clear that the concept of risk has been around for a very long time (Douglas, 1990). As society changed and developed, so too did risk (Frosdick, 1997, p. 175). Various risk analysis methods were developed to analyse the criticality of risks to ensure that those risks posing a serious threat to mostly physical assets and infrastructure could be dealt with by reducing the risk to an acceptable level. Jung et al. (1999, p. 62) backs this statement by defining risk analysis as ''a systematic process to examine the threats facing the IT assets and the vulnerabilities of these assets and to show the likelihood that these threats will be realised''. Thus, traditional risk analysis was a way in which risks to IT assets could be identified and quantified, to determine the probability of risk occurring and the consequence thereof should an adverse event happen causing that risk to materialise. Besides the changes noticed in risk, the changes in society also brought about numerous other advancements such as in the field of information technology (Fung et al., 2003, p. 2). In turn the e-commerce and e-business environment resulted in information becoming such a precious resource (Humphreys et al., 1998, p. 8; BS 7799-1, 1999, p. 1; URN 99/704, 1999, p. 1), that a definitive need for adapting the overall management of risk came about to ensure its protection.

As discussed, the overall management of risk required the process of risk management to be preceded by the process of risk analysis. Traditional risk analysis was very effective for securing assets, such as hardware and infrastructure of which the threats an vulnerabilities could be estimated by means of quantitative/qualitative means (Humphreys et al., 1998, p. 49). If the possibility exists to reach the stage of risk management by some other means besides only relying on risk analysis alone, it is definitely worth investigating. Especially since firstly, preserving information is deemed core to the success of any organisation in the current e-commerce environment and secondly since traditional risk analysis is arguably labelled as no longer being adequate to successfully analyse risks to information assets. Therefore, to protect information, extensive information security requirements of an organisation need to be determined. In identifying information security requirements, more than risk analysis is required.

Understanding information security requirements

Information security requirements are concerned with the amount and specifics of security required for the effective protection of information resources. To ensure that the correct level of information security is obtained to protect information resources, information security requirements need to be determined based on the unique characteristics that each organisation possesses. Although ways in which to analyse risk has been studied by many (Anderson, 1991, pp. 301–311; Baskerville, 1991; Baskerville, 1993, pp. 373–414; Clark, 1989; Garrabrants et al., 1990; Katzke, 1987, pp. 3–20; Birch and McEvoy, 1992; Moses, 1993) it has, however, been claimed that an ideal method, which would suit all organisations does not exist, since each organisation possesses its own unique characteristics (Lichtenstein, 1996, p. 20). This claim supports the need for organisations to incorporate a comprehensive approach for analysing risk, which considers and addresses its unique information security requirements, as an information security requirements analysis intend to do. Besides the critical need for protecting information, there are various other factors that the overall process of management of risk should consider, in order to establish information security requirements.

The foundation of information security requirements

As information includes both technological and humanistic issues, the overall process of managing risk should therefore ideally include factors from both the natural sciences paradigm and the social sciences paradigm (Frosdick, 1997, pp. 169, 175 and 176; Douglas and Wildavsky, 1982; Hartoonian, n.d.). Since traditional risk analysis is seen as being more related to the natural science paradigm, the natural science paradigm is thus already represented in the current ways used for the management of risk. As explained, risk analysis should not be the only determining factor in identifying security controls. Other factors, related not only to analysing the risk to information, but also to the consideration of the social science paradigm should be incorporated to contribute to the overall management of risk.

Based on the assumption that risk analysis is limited to representing the natural science paradigm and that it currently is the only determining factor leading to risk management, the following

question comes to mind. How much more comprehensive and beneficial could the overall management of risk not be if an integrated model could be developed for indicating an alternative approach to risk analysis? The intention is not to replace risk analysis, since risk analysis can still contribute greatly to the overall management of risk. Instead to supplement risk analysis with an approach to address an organisation's unique information requirements for security, while considering issues such as law, politics, economics, history, culture, to name but a few of the social science disciplines to be taken into account.

This proposed view, as explained in the previous section, is backed by an explanation by Humphreys, et al. (1998, pp. 9–10 and 19–20) as well as the British Standards Institute (BSI) (BS 7799-1, 1999, p. 2), which explains three sources of information security requirements. It should be noted that information security requirements are recommended as part of the overall management of risk.

- The first source as described by Humphreys et al. (1998, pp. 9–10 and 19–20) and BSI (BS 7799-1, 1999, p. 2) is derived from assessing the unique set of security risks to the organisation's information systems, which could lead to significant losses in business if they occur. This assessment normally takes the form of a risk analysis that is used for the identification of threats to assets, the evaluation of vulnerabilities to and likelihood of occurrence and estimation of the potential impact.
- The second source is the legal, statutory, regulatory and contractual requirements to which an organisation, its trading partners, contractors and service providers have to comply. Examples of these include the data protection legislation, copyright restrictions and organisational record preservation. Additionally, an organisation may have to adhere to certain contractual requirements, which were drawn up based on relationships when serving as a customer or supplier of products and services.
- The third source relates to the unique organisational principles, objectives, procedures and requirements, developed by an organisation for processing of information to support its business operations and processes.

Recall Fig. 11, which illustrates an overlap between the natural science paradigm and the social science paradigm, with information serving as the link between the two. When observing this illustration, it becomes apparent that all the three elements that it depicts/contains, are also specified by Humphreys et al., as well as BSI as sources of information security requirements. The first source, which deals with the assessment of risk by means of risk analysis, links onto an earlier notion that indicated risk analysis as representing the natural science paradigm. As the social science paradigm includes disciplines such as economics, politics, government, legislation, law, criminal justice, anthropology, culture, ethics, religion, history, geography, psychology, sociology and gerontology (University of Maryland University College, 1996–2003; Central Oregon Community College, 2003; Miami-Dade Community College, 2003; U.S. Department of Labor, 2002–2003; Glenn, 1989–2001), it can be reasoned that it is closely related to the second source, which deals with legal, statutory, regulatory and contractual requirements. Finally it can be contemplated that the third source, which relates to the development of unique organisational principles, objectives, procedures and requirements for supporting information processing, links onto the recommendation that emphasises the need for securing the information resources of an organisation.

Thus, the explanation by Humphreys et al. (1998, pp. 9–10 and 19–20) and BSI (BS 7799-1, 1999, p. 2) of the three sources of information security requirements conforms precisely and accurately to, and is directly in accordance with the deductions made in this document as to which elements were found to be essential for establishing information security requirements. Information security requirements would thus play a major role in the overall management of risk, by analysing risks in a holistic way by utilising a proposed integrated approach, as illustrated in Fig. 12, which considers risks from the natural science paradigm, risks from the social science paradigm as well as risks posed to information, before moving to risk management. Risk management being responsible for reducing risks, faced globally by many organisations today. The need for a holistic approach is supported by a statement made by Peter (2003), the editor of Hi-Tech Security Solutions, who mentions that business continuity depends very much on the use of a holistic approach that includes a carefully planned security policy, the use of technology and well-trained staff.

Conclusion

Risk analysis was traditionally used to analyse risks posing a threat to mostly IT assets (Jung et al., 1999, p. 62). However, with the onset of the

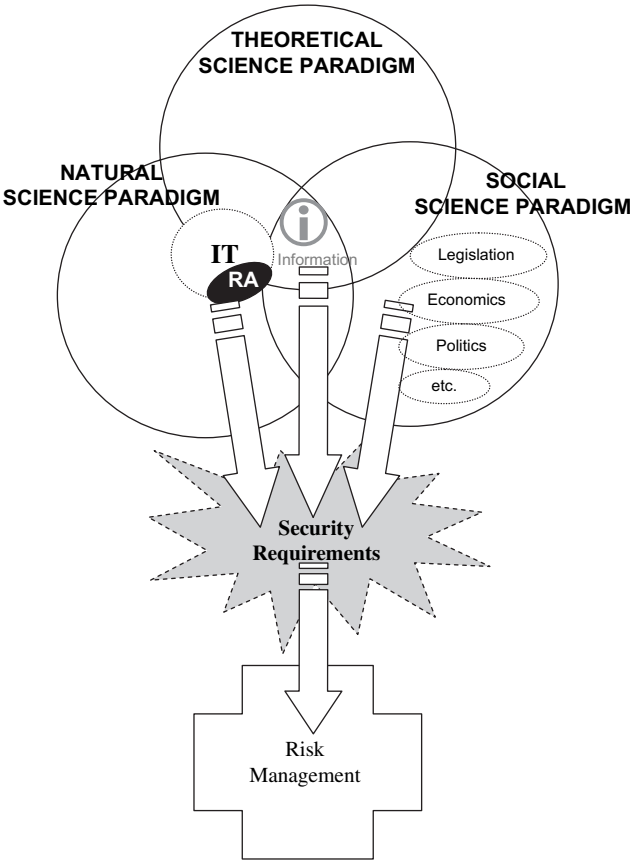

Figure 12 A proposed holistic view of the management of risk.

information age a growing need for protecting information, from risks currently faced by numerous organisations globally came about. As the protection of information is deemed crucial for the continued existence of most organisations (Owens, 1998, pp. 1, 2; Wills, 1991, p. 1), an alternative more comprehensive approach to risk analysis was suggested in this document. This is due the complex and difficult, if not impossible, task of quantifying intangible assets, of which information is an example (Burch et al., 1979, p. 16). Although risk analysis was traditionally used for analysing risk, it focuses mainly on tangible assets (or IT assets as it is called). Resulting in the possibility that the methodology used by risk analysis might not be adequate to ensure the proper protection of information, since it concentrates on one area within the IT spectrum (e.g. technology, hardware and infrastructure). By considering an alternative to risk analysis a holistic view could be gained on the management of risk, moving away from the partial and unrealistic way in which management of risk was done, by searching only within a specific domain (Bandyopadhyay et al., 1999, p. 440). As risk is not fragmented into compartments and silos (Erfmann, 2003), the management of risk should not be either (Smith, 2003). Instead, it is recommended that the entire spectrum related to the IT environment be taken into account, in order to establish the unique information security requirements of an organisation. Information security requirements are concerned with the amount and specifics of security required for the effective protection of information resources based on the unique characteristics that each organisation possesses. This document indicated how information security requirements could be established, using a comprehensive integrated approach that proposes to analyse not only risks to tangible assets, by means of risk analysis, but also risks to information or intangible assets, while considering risks posed due to cultural, legislative and other sociological issues.

References

Anderson AM. Comparing risk analysis methodologies. In: Proceedings of the IFIP TC11 seventh international conference on information security. New York, NY, Amsterdam: North Holland; 1991. p. 301–11.

Bandyopadhyay K, Mykytyn PP, Mykytyn K. A framework for integrated risk management in information technology. Management Decision 1999;37(5):437–44. MCB Press.

Baskerville R. Risk analysis as a source of professional knowledge. Computers and Security 1991;10(8):749–64.

Baskerville R. Information systems security design methods: implications for information systems development. ACM Computing Surveys 1993;25(4):373–414.

Birch DGW, McEvoy NA. Risk analysis for information systems. Journal of Information Technology 1992;7(1).

Boddington T, Hill S. Preparing for BS 7799 certification. London: British Standards Institution; 1998.

British Standards Institution. Quality vocabulary. BS4778 [Part 3 Section 3.2=IEC 1990 50(191)]. London: BSI; 1991.

BS 7799-1. Information security management – Part 1: code of practice for information security management. London: British Standards Institution; 1999.

BS 7799-2. Information security management – Part 2: specification for information security management systems. London: British Standards Institution; 1999.

Burch JG, Strater FR, Grudnitski G. Information systems: theory and practice. 2nd ed. Canada: John Wiley & Sons, Inc.; 1979.

Burnie D. Science. Retrieved Dec 2, 2003, from Microsoft® Encarta® Online Encyclopedia 1997/2003: <http://encarta.msn.com/text_761557105_1/Science.html>; 2003.

Central Oregon Community College. Social science disciplines. Retrieved November 25, 2003 from. <http://www.cocc.edu/admit/shells/trans/social_disciplines.htm>; 2003.

Clark R. Risk management – a new approach. In: Proceedings of the fourth IFIP TCII international conference on computer security. New York, NY, Amsterdam: North Holland; 1989.

Deuchar S. Major organizations take to managing risk. ESecure 2003, March;4. Technews. Retrieved November 04, 2003 from <http://ebiz.co.za/news.asp?pklNewsid=9626&pklIssueID=308>.

Douglas M. Risk as a forensic resource. Daedalus 1990;119(4): 1–17.
Douglas M. Risk and blame. In: Risk and blame: essays in cultural theory. London: Routledge; 1992, p. 3–21.
Douglas M, Wildavsky A. Risk and culture. Berkeley, CA: University of California Press; 1982.
Erfmann C. Are you prepared to share? ESecure 2003, October;4. Technews. Retrieved November 04, 2003 from <http://ebiz.co.za/article.asp?pklArticleid=2095&pklIssueID=286>.
Frosdick S. The techniques of risk analysis are insufficient in themselves. Disaster Prevention and Management 1997;6(3): 165–77. MCB University Press.
Fung P, Kwok L, Longley D. Electronic information security documentation — Australasian information security workshop (AISW2003). In: Johnson C, Montague P, Steketee C, editors. Conferences in research and practice in information technology, 21. Adelaide, Australia; 2003.
Garrabrants WM, Ellis III AW, Hoffman LJ, Kamel M. CERTS: a comparative evaluation method for risk management methodologies and tools. In: Sixth annual computer security conference. Los Alamitos, CA: IEEE Computer Society Press; 1990.
Gerber M, von Solms R. From risk analysis to security requirements. Computers and Security 2001;20(7):577–84.
Glenn JK. Book review: three social science disciplines in Central and Eastern Europe: handbook on economics, political science and sociology 1989–2001;. Retrieved November 25, 2003, from the Columbia University website from page 1 at <http://www.columbia.edu/cu/sipa/REGIONAL/ECE/glenn1.pdf>.
Hartoonian M. Alaska Department of Education & Early Development: making content connections. Retrieved November 25, 2003 from <http://www.educ.state.ak.us/tls/frameworks/sstudies/part2d.htm>.
HSE: Health and Safety Executive. The tolerability of risk from nuclear power stations. London: HMSO; 1988.
Humphreys EJ, Moses RH, Plate AE. Guide to risk assessment and risk management. London: British Standards Institution; 1998.
Infoplease.com. Information please: on-line dictionary. In: Internet Encyclopedia, Atlas & Almanac;. Retrieved Nov 25, 2003 from <http://www.infoplease.com/ipd/A0549812.html>.
ISO/IEC TR 13335-1. Information technology — guidelines for the management of IT security — Part 1: concepts and models for IT Security. 1st ed. Switzerland; 1996.
Jacobson RV. CORA. Cost-of-risk analysis. Painless risk management for small systems. International Security Technology, Inc.; 1996.
Jung C, Han I, Suh B. Risk analysis for electronic commerce using case-based reasoning. International Journal of Intelligent Systems in Accounting, Finance and Management 1999;8:61–73. John Wiley & Sons, Ltd.
Kailay MP, Jarratt P. RAMeX: a prototype expert system for computer security analysis and management. Computers and Security 1995;14:449–63.
Katzke SW. A government perspective on risk management of automated information systems. In: Proceedings of the 1988 computer security risk management model builders workshop; 1987. p. 3–20.
Kirkwood AS. Why do we worry when scientists say there is no risk? Disaster Prevention and Management 1994;3(2):15–22. MCB University Press.
Krupp DA. Introduction to the science of biology: the nature of natural science. Retrieved Dec 2, 2003, from <http://imiloa.wcc.hawaii.edu/krupp/BIOL101/present/lcture01/index.htm>; 1999, July 10.
Lichtenstein S. Factors in the selection of a risk assessment method. Information Management and Computer Security 1996;4(4):20–5. MCB University Press.
Mayo D, Hollander R. Introduction to Part II — uncertain evidence in risk management. In: Mayo D, Hollander R, editors. Acceptable evidence: science and values in risk management. Oxford: Oxford University Press; 1991. p. 93–8.
Merriam-Webster's collegiate dictionary. Merriam-Webster Incorporated; 2002.
Miami-Dade Community College. Social Science Department: disciplines. Retrieved November 25, 2003 from <http://www.mdcc.edu/kendall/social/disciplines.htm>; 2003.
Moses RH. Risk analysis and management. In: Jackson KM, Hruska J, editors. Computer security reference book. Oxford: Butterworth-Heinemann Ltd.; 1992.
Moses R. A European standard for risk analysis. In: Proceedings of COMPSEC international. Oxford: Elsevier; 1993.
NIST (National Institute of Standards and Technology). An introduction to computer security. [Special publication 800-12]. Washington: U.S. Department of Commerce; 1995.
NIST (National Institute of Standards and Technology). Risk management guide for information technology systems. [Special publication 800-30]. Washington: U.S. Department of Commerce; 2001.
Original Roget's® thesaurus of English words and phrases. 5th ed. Essex, England: Longman Group UK limited; 1992.
Owens S. Information security management: an introduction. London: British Standards Institution; 1998.
Oxford advanced learner's dictionary. 5th ed. Oxford: Oxford University Press; 1995.
Peter G. SA must be ready for a new threat. ESecure 2003, July;4. Technews. Retrieved Nov 04, 2003 for <http://securitysa.com/regular.asp?pklRegularid=1435&pklIssueID=340>.
Pfleeger CP. Security in computing. Englewood Cliffs, NJ: Prentice Hall; 1989.
Pfleeger CP. Security in computing. 2nd ed. Prentice Hall, Inc.; 1997.
Priest G. The new legal structure of risk control. Daedalus 1990; 119(4):207–28.
Roth G. E-commerce and e-business have changed the profile of corporate legal risk. ESecure 2003, September;3. Technews. Retrieved Nov 04, 2003 from <http://estrategy.co.za/news.asp?pklNewsID=12125&pklIssueID=346&pklCategoryID=141>.
Royal Society. Risk assessment, report of a Royal Society study group. London: The Royal Society; 1983.
Royal Society. Risk: analysis, perception and management, report of a Royal Society study group. London: The Royal Society; 1992.
Scarff F, Carty A, Charette R. Introduction to the management of risk. Norwich: HMSO; 1993.
Smith D. Major organisations take to managing risk. ESecure 2003, March;4. Technews. Retrieved November 04, 2003 from <http://ebiz.co.za/news.asp?pklNewsid=9626&pklIssueID=308>.
Smithson M. The changing nature of ignorance. In: Handmer J, Dutton B, Guerin B, Smithson M, editors. New perspectives on uncertainty and risk, Centre for Resource and Environmental Studies. Mt Macedon: Australian National University, Canberra and Australian Counter disaster College, Natural Disasters Organization; 1991. p. 5–58.
Stark H. Engineering. Retrieved Dec 2, 2003, from Microsoft® Encarta® Online Encyclopedia 1997/2003: <http://encarta.msn.com/text_761570676_1/Engineering.html>; 2003.
Strutt J. Risk assessment and management: the engineering approach. Unpublished paper, Centre for Industrial Safety and Reliability, Cranfield University; 1993.

Suojanen T. Technical communication research: dissemination, reception, utilization. Unpublished Licentiate Thesis in translation studies: English translation and interpretation. Retrieved Dec 2, 2003, from University of Tampere Web site: <http://tutkielmat.uta.fi/pdf/lisuri00001.pdf>; 2000.

Tchankova L. Risk identification — basic stage in risk management. Environmental Management and Health 2002;13(3): 290—7. MCB UP Limited.

The American Heritage® dictionary of the English language. 4th ed. Houghton Mifflin company; 2000.

University of Maryland University College. Social science: supplemental major courses. Retrieved November 25, 2003, from University of Maryland University College Web site: <http://www.umuc.edu/prog/ugp/majors/socs.shtml>; 1996—2003.

URN 99/704 (NEW). Information your most valuable asset. Protect it. Department of Trade and Industry; 1999.

U.S. Department of Labor. Bureau of labor statistics: occupational handbook. Online. http://www.bls.gov/oco/home.htm; 2002—2003.

Warner F. Calculated risks. In: Science and public affairs winter 1992; 1993. p. 44—9.

Weems BS. Computer science. Retrieved Dec 2, 2003, from Microsoft® Encarta® Online Encyclopedia 1997/2003: <http://encarta.msn.com/text_761563863_1/Computer_Science.html>; 2003.

Wikipedia. Wikipedia: the free encyclopedia. Retrieved September 8, 2004 from. <http://en.wikipedia.org/wiki/Natural_science>; 2004, October.

Wills M. Personal communication. In URN 99/699 (New). Protecting business information — overview. Department of Trade and Industry; 1999.

WordNet® 1.6. Engineering. Princeton University. Retrieved November 26, 2003 from. <http://dictionary.reference.com/search?r=2q=engineering>; 1997.