Global Information Assurance Certification Paper

The security gap in risk analyses

Differences in the application of risk analyses between (IT-)security people and managers.

Serge van der Schaft
28 februari 2005

GIAC Security Essentials Certification (GSEC)
Practical Assigment (version 1.4c)
Option: 1 – Research on topics in Information Security

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

Information security has been talked about for quite a while and has been organised around risk management. There are many different tools, methods and technological solutions to support risk management and analyses. In general these supports can be divided into two groups: suitable for managers and suitable for IT(-security) people. In this paper the existence is shown of a security gap in the way managers and IT(-security) people handle risks, followed by the problems that are caused by the gap. Next the causes for the gap are investigated by pointing out the differences between the two groups and by grouping important causes of the gap into four categories (technological, business/organizational, legal and societal). Then suggestions to overcome the gap are given, as well as a short path. One conclusion is that this paper is a good start in overcoming the gap.

Contents

Introduction

The usage of information in our society has constantly been rising. So has the value of information. Nowadays, most information cannot be produced without computers. But remember that these machines in commercial usage have only been around for four decades. The rapid growth of both the complexity of computers and the importance of information for the continuation of companies has led to a lot of miscommunication between managers and IT personnel concerning risk management. This miscommunication leads to a serious security gap in risk analysis, which is the subject of this paper.

Let us start with some history of computers and information. In the sixties, it took years of education and high technical skills in order to be able to interpret the results of a computer. The results had to be explained to managers and managers had to make clear which information they wanted. Ever since, computer languages have been made easier so that it is less necessary to have the highly trained skills to be able to interpret the computer results. Besides, general education has brought society more general computer knowledge.
The very essence of computers did not change, but computers became technically more complex. This has increased again the demand for highly trained people. Developments in computer science and in the computer industry have gone much faster than the computer education rate of society. On the other hand one can see that there are some people who get a competitive advantage by only using computers for their specific business, like Amazon.com, and there are even signs of news business patterns (Brynjolfsson, 2002). More and more people are needed to help society handle computers. This also means that the society hardly knows what issues and particular difficulties the usage of computers implies.

During the last decades, the value of computers to produce information has been recognised. A market for information has been created, with supply and demand, with abundance and scarcity. As a result, a whole new part of society has been created. Information has become a value factor on itself. One can even go as far to say that information has become another production factor for companies. Besides the traditional production factors as capital, natural resources and people, information has become an essential factor in creating value. Irrespective of the produced results, the value of information has changed dramatically in the last decades, much more than the value of the other production factors.

Sooner or later, anything that represents value has to be protected. There is one big difference, however, between the traditional production factors and information. The traditional production factors are tangible and visible. Capital, natural resources and people can be kept hold of. That means that these can be physically contained or restricted. Information, however, is (in itself) not tangible. Information is nothing more

than a message: a message that is carried on a medium. A medium could be for instance paper, electricity, light or air. At most the medium that carries the information is tangible, but even that is sometimes not the case as with electricity or light. For the protection of the production factor 'information' this creates huge problems.

As stated above, relatively valuable information has to be protected. This is the very same principle that has been around for ages: anything that represents value has to be protected. Else, sooner or later, there will be people abusing the non-protected items. The point is, what is the value of information?
Information does not have equal value. Some information is more valuable than other. There are several ways to determine the value of information. One way to determine it is by calculating the monetary value of information. Other ways are to determine the information that has the highest threats, or, in case of vandalism, information that is easiest to disturb.

Summarizing,

- the complexity of computer systems has grown rapidly, so IT-engineers are required for the technical issues, and
- the value of information obtained through the computer systems has increased rapidly, giving managers the task to protect the information in order to protect their business.

However, the different tasks and points of view of both the engineers and the managers result in a 'security gap' concerning the protection of information. This gap is a serious threat for the continuity of businesses.

In the following of this paper I start with a more detailed introduction to the protection of information and the related risk analysis and risk management. Then, in Chapter 3, the security gap is described and it is explained why this is a problem with respect to risk analysis. In Chapter 4 I describe the causes of the gap and in Chapter 5 I give a number of ways to fill the gap. I conclude this paper with my conclusions.

Risk analysis and risk management

Organizations want to protect their assets in order to survive. The more a production factor contributes to reaching the goals, the higher the value of that production factor. As mentioned in the introduction, information is an essential production factor, besides labor, capital and (natural) resources.

In the early days of using computers to process data, only specially educated people knew how to operate computers. The costs of the computer itself provided reason to protect the machine. In the beginning protection of the machine meant only controlling physical access. The group of people that had enough knowledge to operate any part of the machine was small. Furthermore, computers were not yet widely connected to each other and if they were, most people were aware of the fair use of the various machines.
Nowadays computers are widely interconnected. Open standards have created the possibility to access a computer for very specific purposes. Computers even access other computers for various reasons. About every (formalized) decision process can be modeled into a computer program. Furthermore, the amount of parties involved steeply rose, namely, it got necessary to involve specially educated people to get certain tasks done (like producing and assembling the right hardware, setting up the machines, installing the software on the computer, implementing the business process and keeping the system up and running). The fact that more parties have to work together also creates possible gaps in the process of getting the computer to work right and secure.

Risk management

Almost everyone uses risk management in real life. Whether you shut your front door (or not) is an example of balancing the perceived threat to the amount of energy you have to (or want to) put in to shut the door. And whether you just close the front door or lock it is another risk management situation.
For companies this is the same. The front door of the company is often well guarded. It is supposed to welcome wanted people, while the guard has been put in place to keep the unwanted people out. To extend this example somewhat further: unwanted people who really want to get in are often successful by trying backdoors. From the managers point of view not all backdoors are equally vulnerable. Backdoors on first floors are usually a little harder to find or to open from the outside.
Just like the doors, managers also have the task to protect the information. Computers also have front and backdoors. Remember, however, that buildingdoors represent physical things. Information is not tangible. Doors on computers are just an analogy to make things more clear to non-technical people.
This means that risk management for information is not tangible and therefore more complex and harder to understand.

To get more precise, risk management is a systematic way to handle risks. Risks management with respect to information has been defined several times. To name just two:

- the management of risks that threaten the automated processing of data and the information supply [Looijen, p. 92], or
- (enterprise) risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. [COSO, p. 2]

In short one could say that everyone has the objectives to be certain about the way his/her process goes (a process is a sequence of actions and closely connected to achieve the objective of the person), which means that one must know what happens if random input is thrown into his/her process. Therefore, the ideal situation is that all possible ways to disturb a process must be known and counteractions must be known to as well. Off course, this is impossible.

In some methodologies risk management is inherently combined with risk analysis. Risk analysis is the systematic recognition, inventory and evaluation of actions, measures against possible occurrence of unwanted events. In fact, a good risk management methodology does not go without some form of risk analysis.

Risk management comprises of the systematic risk analyses that are carried out. Risk management is used to balance the costs and the benefits to the threats that potentially encounter the organisation. Some examples of methodologies that comprise risk management are:

- Enterprise Risk Management Framework (COSO 2),
- Control Objectives for IT and related Technology (Cobit),
- Code of Practice of Information Security Management (BS 7799), now more or less turned into ISO 17799:2000,
- ISO 13335, Guidelines for the management of IT security (GMITS),
- Risk management guide for information technology systems, NIST special publication 800-30,
- Common IT-security practises, NIST special publication 800-14;
- Common criteria,
- General Accepted System Securrity Principles (GASSP),
- Information Technology Infrstructure Library (ITIL),
- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE),
- CCTA Risk Analysis and Management Method (CRAMM),
- Code Tabaksblat.

These examples are taken from Le Grand (Le Grand, 2002) and Oud (Oud, 2004).

GAP

In this chapter first the meaning of the gap is explained. Then some ways one can notice the gap are shown, followed by the problems that are caused by the gap and finallay the chapter concludes by giving causes for the gap.

What is meant by the gap?

Today's society uses risk analysis to balance threats and measures to ensure the security of information. Every protective measure costs money and raises the bar in handling information.
The question is of course how effective the measures are relative to the costs.

As computers used to be the area of IT-engineers, the security of computers also was the area of engineers. Engineers had a technical education, so the protective measures were also based on (limiting the) technical possibilities.
Over the years computers became more complex and the needed technical knowledge to protect computers had grown exponential. The engineers realized that one small insecure aspect of the computer could potentially put the whole computer at risk, data and information included.
When potential vulnerabilties interact with other potential vulnerabilities and the amount of vulnerabilties grows, the process to keep computers secure becomes more and more complex. And thus the process of balancing (technical) threats and (technical) protective measures became more and more complex. Adding the growing organisational complexity might lead to an overwhelming complex situation where it is impossible to have an overview on security.

In order to be able to protect all technological security issues, some organisations like the NSA and CERT created supporting tools for specific applications (pun intended) like the Router Security Configuration Guide (Antoine, 2001) and the Unix security Checklists (Cert, 2001). These guides are very detailed and provide support for IT-people. The guides were not not suitable at all for managers because of the technological knowledge needed and the high level of detail. Admitted, this document was only intended for IT-people.

Managers realized that computers (only) helped them in getting the information they wanted to run their business (process). Of course, the information with high value had to be protected. For instance, one does not protect information that is one hundred euro worth with protective measures that costs the company one thousand euro.

So for business managers other tools & risk methodologies were developped. These tools and methodologies were high level: aimed at non-technical & general useability. The Sprint methodology of the Information Security Forum is an example.
In this methodology the user is given twentyfour questions about availability, integrity and exclusivity that can be understood by every procesowner (Oud, 2004).

Besides, becuase of the several accounting frauds, the governance of companies by C-level executives was questioned. New frameworks were introduced together with new laws. COSO-Enterprise Risk Management, Sarbanes-Oxley and HIPAA were introduced in the US.
In many cases IT-security is treated as a part of IT-governance and on ISACA's mailing list about IT-governance participants regularly agree on this.
So now managers also had the explicit responsability for IT-security, but from another background and point of view as the traditional IT-security responsability (the engineers).

Here another problem was created. Although aimed at managers, the amount of reading material was in some cases simply too much. Most of the frameworks are about 100 pages. This holds for the Control Objectives for IT and Related Technology (Cobit, 2000), but also for the more community driven organisation like IETF, that developped RFC 2196, the "Site Security Handbook (Fraser, 1997). Or the The Forum's Standard of Good Practise from the Information Security Forum (ISF, 2000).
In the Netherlands, the (translated) code of practice for information security management was often used (Oud, 2004).

Some companies managed to translate a framework into their own policies, but even then the text could be interpreted in various ways. IT-security people felt they had to make another translation into the technical domain (not seldom without having to give account to someone else). This led to the same result that managers could not bear their responsability well. And IT-security people could not get their point accross.

Another factor that widens the gap is the (geographical) extensivenes of technology and legislation. The technology that is used in (for instance) the Netherlands, is the very same technology that is used anywhere else in the world. With respect to technological actions, IT-people can work anywhere in the world.
However, the legal aspects are not the same. In the Netherlands there are some companies that have to abide by some American laws. The American laws are different from Dutch laws, or European Union legislation. There is for instance a Dutch (less far reaching) equivalent for Sarbanes-Oxley, called Tabaksblat, but most companies in the Netherlands are not (yet) subjected to this governance laws. For security, the Dutch privacy protection law is a good driver, though (CBP, 2001).

In daily life these two different viewpoints exist side by side. Managers look at protecting the companies' assets differently than information security professionals do. There is usually not a lot of understanding between the two groups.
IT-educated people are usually more technology-risks based and managers are usually more general and asset-risks based.

How is the gap noticed?

In daily life this gap is noticed about every time that business managers and IT people talk to each other about security. This might not be often the case. Business managers sigh that IT-people are not willing to cooperate and IT-people complain that business managers do not know what they are talking about because of a lack of knowledge. In other situations, it might well be the case that the gap between IT-security people and business managers can be called ignorance. (Rapoza, 2003).
The result is that IT-managers find themselves in the hopeless situation of trying to uphold a maximum of security, as requested from management, while at the same time they are considered an obstacle in the way of developing and introducing new applications into industrial, business and government network environments (Lubich, 2000).

In the last decades, user interfaces became more standardized. Microsoft and Apple have done a tremendous job by standardizing the user interfaces into graphical environments. Standardizing these interfaces also gave users the impression that operating a computer was not so hard that one always needed engineers. One of the consequences was the idea that if one could work with a computer at home, one could work with them at home. However, lack of networking knowledge could bring down a whole company network, by simply clicking around. Just because “it is just like at home”.

On the other hand, if managers take the lead in information initiatives, the translation from general company wide policies on IT-security, causes interpretation problems with IT-security people.
For example, simple and common statements like “all access to data has to be controlled” causes problems in a technical context. It also means that automated (system) logins (for example necesarry for nightly back-ups) have to be controlled, (all) logins over the network as well (which accicdently might or might not be the same as the previously mentioned automated system logins). And does retreiving a webpage also mean accessing data?
Various IT-security people interpret the generally stated policies in various ways. So even among the (technical) specialists, there is no common understanding. One could go as far to say that every plain English (or Dutch) sentence, whether it be a policy line or a part of a risk analysis, can be interpreted in lots of different ways.
How then could a manager lose his ignorance?

Why is the gap a problem?
The gap is a problem because when security is left to any of the groups, be it either the IS people or the managers, a false feeling of information security is created. This (false) feeling does reflect the balanced interests, so it does not protect against the threats that each group sees.
According to Andrews the organization is therefore:
- not fully aware of the information security risks to their operations,

- accepting an unknown level of risk by default,
- unconsciously deciding what level of risk was tolerable,
- relying on ineffective controls,
- deal with security issues on an ad-hoc basis,
- not able justify the spendings on security.

(Andrews, 2003)

Although many security frameworks and techniques are available today, the overall security situation in many, networked organizations is far from acceptable. (Lubich, 2000).
Soohoo has demonstrated in his decision analysis model the relative importance of different input variables and assumptions. He concludes that the current level of reported computer-security related risks warranted only the most inexpensive of additional safeguards. (Soohoo, 2000).
This very reason is the justification to focus this paper on the existence of the gap. Up to today, in my own practise this gap costs me much energy. Therefore I do not focus on one tool, methodology, technique or technological solution.

What causes the gap?
The false feeling of security has various causes and can be looked at in various ways. First I'll give some explanations that I see in reality and second I present some additional aspects that are categorized by Lubich.

First there are differences in interests, language, education, uncertainty, knowledge, detail of view, view on (process) controls and methods to handle information (in)security.

- There are differences in interests.
  It is in the interest of managers to have an overview on the value that is added in a process. Reaching companies goals and objectives is their responsibility. Details are not their kind of thing. Security is almost never a value adding process and hinders them in reaching their goals.
  IT-security people are hired to protect information. As they know that they are hardly able to protect the information itself, they have their protections measures aimed at people, processes and technology. Often technology receives the most attention as most IT security people have a firm background in technology.
- Another cause is the difference in language that is spoken by the two groups.
  It might be a big difference hearing a manager talking about a 'system', compared to an IT-security person talking about a 'system'. A managers speaking about a control might mean something completely different than an IT-security person means with a control. And how secure is secure? Is it safe? The basics are just not well defined nor commonly agreed upon between the two groups.
- And there are differences in education.
  IT-security people often have a firm background in IT. They should know the

techniques that make the system work. Managers are usually not educated in IT. They usually know their process, which is the functional side of the application layer, but that does not mean they know how the applications really works.
- In case of uncertainty, managers could turn to other IT-people to get a second opinion. However, these other IT-people could well not be able to judge security assertions.
- Non-IT-security people often have the impression that IT-security people are blocking their way (and vice versa). Non-IT-security people often have to reach a functional goal, often under time pressure and IT-security people can slow down their process.
- The granularity of the view is different.
  IT-security people know that the devil is in the detail. The security of an IT-solution is the resultant of all previous work that has be done. This means that an IT-security person needs to check all aspects of a solution in order to conclude that something is (in)secure. Which could mean that a whole process has to be done again. Managers usually lose interest when it comes down to details. They find it hard to understand that a single piece of information potentially can break down a whole building (with respect to information security).
- IT-educated people think that the process controls often correspond with security controls in the application.
  Managers think of process controls differently. Security controls to them are just one type of controls. They know the four eyes principle
- An overflow of methods to handle/balance information security effectively. Knowing the best methods well asks too much effort of the IT security people and there are just too many models to choose from accounts for the manager.

In the next section I draw on Lubich's exploration and categorization:
Lubich states that the commonly perceived problems are technological shortcomings, business/organizational aspects, legal/regulatory pitfalls or societal issues (Lubich, 2000).

Technological shortcomings
Many shortcomings of IT security elements have their roots in technological problems:
- There are too many encryption systems and products that do not work together.
- A general infrastructure with built-in trust capabilities is under construction. (Mazzeo, 2004)
- An unsettled debate as to which security services should be provided by which functional layer (network, operation system, middleware, application, presentation).
- The (very) large number of components and corresponding dependencies create an additional level of complexity, which has hampered a common security platform.
- Proprietary supplied frameworks (such as SAP) utilize their own 'embedded' security modules and methods, that may or may not work together with existing systems and frameworks.

- The complexity and openness of interfaces between the organizations and entities in the outside and untrusted world hinder a coherent security environment.
- Existing, legacy systems cannot be integrated into a 'new' one security framework.
- The existence of bugs and deficiencies in IT-security software, as well in particular configurations.

Business/ Organizational aspects

- The roll of IT-security is often perceived as an obstacle for the implementation of new business applications
- The non-delegable responsibilities of organization's executive boards as defined in corporate laws makes senior managers over-sensitive in terms of decision making
- Many organization do not delegate sufficient executive powers for the IT-security organization to ' pull the plug' if necessary.
- The outsourcing of parts of the IT services adds to the complexity of detecting and repairing security problems
- There is a growing need for security specialists (the right level of specialization and business understanding)
- Operational risk management has only just taken off (mostly under pressure of governance laws like Sarbanes-Oxley) and information security is just one item to be addressed.

Legal/regulatory pitfalls

- Various countries have various laws about data protection and (computer-)audit requirements may complicate in an international company
- Export/import controls on security technology have delayed the introduction of high-quality (IT-)security products. In the nineties the US government found it necessary to restrict the usage of 128 bit encryption technologies.

Societal Issues

- in many countries there is an open debate on issues of informational self control versus the right for extensive "data mining" by companies using (and extending) their customer information bases by exchanging them with other companies or marketing organizations.
- It is difficult for many people to determine an acceptable level and consistent method of risk-taking – many operational IT-risks do not compare well to risks known to the average person, thus making it difficult to build the required expertise (based on inevitable but expensive errors and misjudgment)

Suggestions

It is in the interest of all parties to bridge the gap. However, as Charles Le Grand said: "there are no easy solutions" (Le Grand, 2002).

There are already many methods and tools that possibly can help. To reduce the uncertainty all parties should have an agreement and understanding on the tools and method applied.
In my opinion, the risk management methods that I already mentioned briefly in chapter two can work out well, as long as they are interpreted (and acted upon) as communication frameworks.

Only then the discussion between managers and IT-security people can begin:
- Educate managers to know more about the technological problems. Managers should be taught a structure in order to judge whether information security issues could become important.
- IT-security people could make more use of analogies to make IT-security arguments clear (or to 'proof' the reverse). In my own experience the analogy with the automotive industry is quite often useable.
- Educate IT-(security) people to apply a risk management framework.
- Educate IT-security people better in calculating the cost of IT-security measures [Soohoo, p2.] An example of this is the calculation is the Return on Investment (ROI) for penetration testing. (Wilson, 2003).
- Educate managers better in calculating Return On Security Investments (ROSI). (Berinato, 2002).
- Communicate each other interests more clearly. This will take time and it may be that managers are not willing to spend this time, because it is not directly contributing to earnings and profits. There have been some initiatives to create a market for information security (Landwehr, 2002).
- Create a settlement procedure in case a manager has a conflict with an IT-security person. And also a settlement procedure in the reverse case.
- Learn to interpret the language of the other group. Managers are usually more sensitive for language nuances, where IT people might be less sensitive to language. Managers might love (critical process) indicators, where IT-security people trigger on certain events.
- Re-educate in the other field of interest. A very drastic solution, but surely one that can help. The drawback is that not everyone is willing to do this.
- Put someone (with knowledge of both fields) in between the manager and the IT-security people. IT-Auditors with a firm technological background should be able to build bridges (Le Grand, 2002).
- Put responsibility for information security in the hands of professional risk managers.
- Develop new methods that give good graphical insight in data and security

dependencies [Soohoo, p. 5]. Graphical presentations of IT-security data help to communicate the problems better.

Conclusion

In this paper I have tried to communicate an underexposed issue of information security: the gap between IT-security people and managers in the way they handle risks. I have shown that the existence of the gap is reasonable and might lead to ignorance and a false sense of security. The gap in information has various causes. Because information security itself is not an easy subject, overcoming the gap in the way information security is handled is an even bigger challenge.
Managers should not be overloaded with information about information security and IT-security people should be well aware of the way businesses are managed.
One way to overcome the gap is by choosing a risk management framework.
By understanding possible misconceptions between the groups first and then starting a discussion to handle information security is a good way to overcome the information security gap. In that way a risk management method can serve as a common communication framework.
This paper might therefore be a good beginning to start understanding the misconceptions between the two groups.

References

Andrews jr., A.D.; “Security program management and risk”; March 23, 2003; http://www.sans.org/rr/whitepapers/auditing/1061.php

Antoine, V., Bismajian, P., et al.; “Router Security Configuration Guide”; National Security Agency (NSA); April 20, 2001; Version 1g; http://nsa1.www.conxion.com/cisco/download.htm

Berinato, S.; “Finally, a real return on security spending”; CIO Managzine; Feb. 15, 2002; http://www.cio.com/archive/021502/security.html

Brynjolfsson, E., Kahin, B.; “Understanding the digital economy”; Massachusetts Institue of Technology; 2002; ISBN 0262523302

CBP; “Samenwerkingsverband Audit aanpak”; 2001; College Bescherming Persoonsgegevens; http://www.cbpweb.nl/structuur/pag_audit.htm

CERT; “Unix Security Checklist v2.0”; CERT Coördination Center; 10-10-2001; http://www.cert.org/tech_tips/usc20.html

Cobit (Control Objectives for Information and Related Technology), “Management Guidelines”; IT Governance Institute; July 2000; http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Obtain_COBIT.htm (freely available after creating a login account)

Coso (Committee of Sponsoring Organizations of the Threadway Commission), “Enterprise risk management – integrated framwork”, Executive summary - draft, September 2004, AICPA; http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

ISF; “The Forum’s Standard of Good Practise, the standard for information security”; November 2000; Information Security Forum; http://www.securityforum.org

Landwehr, C.E.; “Improving information flow in the information security market”; Workshop on Economics and Information Security; May 16-17, 2002; University of California at Berkeley; http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt

Le Grand, C.; “Pressures changing the audit profession”; IT-audit; June 1, 2002; http://www.theiia.org/itaudit/index.cfm?fuseaction=print&fid=451

Looijen, M.; Beheer van informatiesystemen; 1998, Kluwer Bedrijfsinformatie b.v.,

Deventer; 3e herzien druk; ISBN 902672800X.

Lubich, H.P.; “The changing role of IT-security in an Internet World, a business perspective”; May 22-25, 2000; http://www.terena.nl/conference/archive/tnc2000/proceedings/2A/2a2.html

Mazzeo, M.; “Digital Signatures and European Laws”; January 12, 2004; http://www.securityfocus.com/infocus/1756

Oud, E.J.; “Risicoanalyse; het doel, de methodieken en het uitvoeren van audits”; EDP-auditor; Reed Business Information BV; nr 3 2004; p 24-30; http://www.norea.nl/download/EDP3_2004.pdf

Rapoza, J.; “Technet fights security ignorance”; december 8, 2003; http://www.technet.org/cybersecurity/itn_eweek_1/ or http://www.technet.org/article/0,4149,1407903,00.asp

Fraser, B., “Site Security Handbook”; 1997; IETF Request for Comment 2196; http://www.ietf.org/rfc/rfc2196.txt?number=2196

Soohoo, K.J.; “How much is enough? A risk management approach to computer security”; working paper ; Palo Alto, CA: Center for Interantional Security and Cooperation; 2000; http://cisac.stanford.edu/publications/11900 or http://cisac.stanford.edu/docs/soohoo.pdf

Stoneburner, G., Goguen A., Feringa, A.; “Risk management guide for information technology systems”; NIST special publication 800-30; 2001; http://csrc.nist.gov/pubications/nistpubs/800-30/sp800-30.pdf

Wilson, M.J.; “Demonstrating ROI for penetration testing”; August 3, 2003; http://www.securityfocus.com/infocus/1718