Eric Piepers
GSEC Practical Assignment Version 1.2e
June 6, 2001

Cost-effective Information Security

(Information Security from a business perspective)

Introduction

During my work as an ICT Security Officer for a global ICT service provider I've always had to deal with the financial aspects associated with the security of information services supplied to customers.

From this background I can without doubt make the statement that information security generates costs and thus requires financial resources, i.e. a budget.
These budgets, apart from being one of the main enablers in implementing and managing information security are also at the same time one of the main limiting factors.

Budget constraints demand cost-effective information security!

This paper is intended to provide security professionals and their management food for thought and information about the issues and areas surrounding cost-effective information security. Technical security professionals should be aware that cost-effective information security facilitates them in doing a good job. This is why I knowingly have written this non-technical paper towards a mainly technically oriented community. Having said this I hope that those security professionals that take up the challenge to read this document are also willing to pass it on to their management.

The information in this paper is based on the deployment of, and information from mainly European standards for information security management [1] while sometimes looking at the "Control Objectives for information and related Technology" [2] from the IT Governance Institute. Other online resources used are Cert and NIST publications[3].

Business perspective

To achieve their goal organizations formulate business objectives and try to achieve these objectives by means of business processes. For the execution of these business processes organizations are nowadays highly dependent on information and associated Information Technology (IT) services. Anything that threatens these Information Technology (IT) services (i.e. the information or the processing of that information) will directly endanger the performance and thus business objectives of the organization.

As a consequence Information security, i.e. the protection of information and information processing facilities is currently widely accepted as a means of achieving business objectives.

[1] ITIL, BS 7799-1 and BS 7799-2
[2] CobiT
[3] OCTAVE and RMG

Organizations create budgets to achieve their business objectives. But it will have a negative impact on the organizations competitive edge if these budgets are overrun. In the successful realization of their business objectives are organizations thus constrained by their budgets.

> Cost -effective management of business processes, information, Information Technology (IT) services and hence information security is essential for both the competitive edge and survivability of an organization.

Effective information security

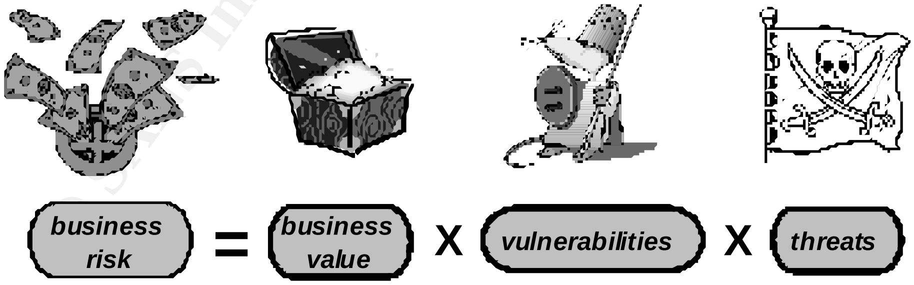
Effective information security should be driven from a business perspective; i.e. security measures should match the need. This implies that next to the *need for information security* not only the *costs of information security measures* but also the *added value of the implemented information security measures* should be evident.

In other words organizations must know their needs, be well aware of what they buy and know what the associated costs are. This is unmistakably one of the true challenges of effective information security management.

Need for information security

The need for security must be based on the business risk and the business risk should be identified by a risk assessment. But what is business risk, what is a risk assessment, and what is the added value of a risk assessment?

Business risk.
Business risk is the likelihood that a threat due to the existence of a matching vulnerability materializes into a security incident causing damage to the information and/or Information Technology (IT) services of an organization. The significance of the damage depends on the business value of assets affected and the impact of the security incident.



What is business risk?

The following statements about the business risk are derived from the ‘formula’ shown above:

1. The absence of threats (threats = 0) implies the absence of business risk.
2. The absence of vulnerabilities (vulnerabilities = 0) implies the absence of business risk.

Based on the above we may conclude that:

- Security measures should focus on the mitigation of vulnerabilities and threats, i.e. the mitigation of risk.
- The most significant business risk is imposed by Information and IT services having high business value and those that are exposed to significant risks.

Risk assessment

A risk assessment should be aimed at identifying information and IT services of major business value or that are exposed to significant risks.

An inventory of information and IT services that are exposed to significant risks or that are of major value to an organization will provide the base for an overview of the need for information security within an organization.

Such an inventory enables management to focus and set priorities in taking decisions about what areas require security attention and the level of information security required.

Costs of security

Not all information and IT services are of equal importance to an organization or exposed to the same level of risk. The cost of information security should therefore be appropriate to the importance of the information and/or IT services and the level of risk exposed.

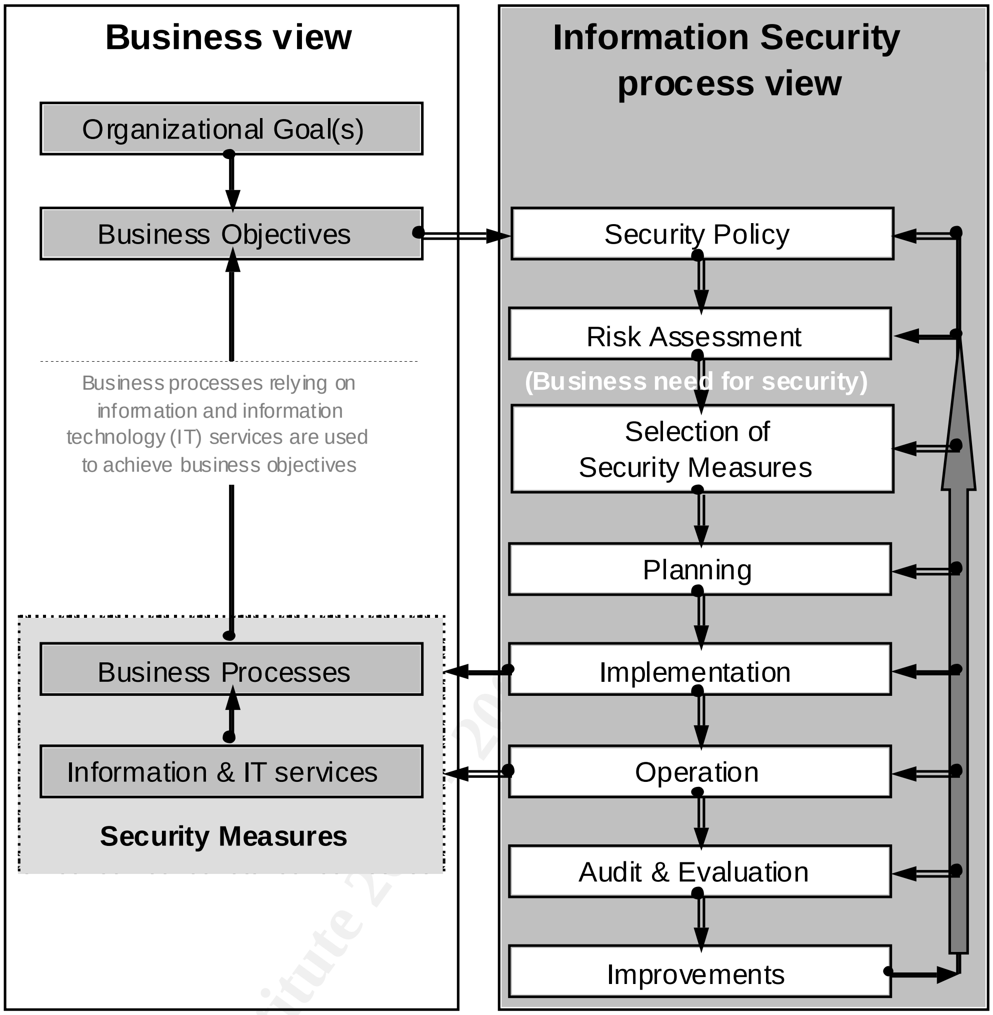
There certainly will be cases where the cost of information security is not appropriate but exceeds the importance of the information and associated IT services. In such cases organizations will be faced to accept the security risks and thereby the costs associated with security incidents when those occur.

The above underlines that information security should be driven from a business perspective.

The implementation of effective security requires management to take decisions on which security measures to implement and which not. To take this decision the management, next to risk assessment information (what is of high value, what is exposed to significant risk) also needs to know the costs of the security measures to be taken. Knowing the costs of security measures a/o requires having a complete overview of the cost elements associated with the implementation of security measures.

Effective and efficient information security requires security measures to be an integral part of business processes. The iterative management (i.e. the principle of plan, do, check, correct) of business processes is commonly accepted as good (or best) practice. As such it should be obvious that also information security being a part of business processes must be managed as an iterative process that requires a proper organization.

The following picture provides an overview of the elements in an Information security process generating costs.


Business view
Organizational Goal(s)
Business Objectives
Business processes relying on information and information technology (IT) services are used to achieve business objectives
Business Processes
Information & IT services
Security Measures
Information Security process view
Security Policy
Risk Assessment
(Business need for security)
Selection of Security Measures
Planning
Implementation
Operation
Audit & Evaluation
Improvements

Information security process cost elements:

- <u>Security policy</u>
  The security policy should be derived from the business objectives and be further specified (in reducing levels of abstraction) in guidelines, processes, procedures and work instructions).
- <u>Risk assessment</u>
  Risk assessment is necessary to identify the organization's security needs.
- <u>Selection of security measures</u>
  The selection of security measures to address the organizations security needs is the process step where the decision about the cost effectiveness of security measures is taken. Only cost-effective security measures should be implemented. The organization should accept the risks associated with those security needs for which no cost-effective security measures can be realized.
- <u>Planning of selected security measures</u>

For selected security measures the planning of implementation of security measures includes all process steps from policy till improvement!

- Implementation of security measures
  The implementation of security measures includes items like the implementation of security tooling, the setup of the organization and the development and documentation of processes, procedures and work instructions.
- Operation of security measures
  The operation of security measures encompasses the execution of the day to day operation of security measures, e.g. authentication and authorization management, security log evaluation and the maintenance of security tooling.
- Audit and evaluation
  The measurement and reporting of the effectiveness and efficiency of security measures. This should be based on key performance indicators reflecting both the *efficiency* (cost of security) and *effectiveness* (match the needs) of security.
- Improvements of any of the security process elements
  Improvements to any of the security process elements should be based on the information from the audit and evaluation process step.

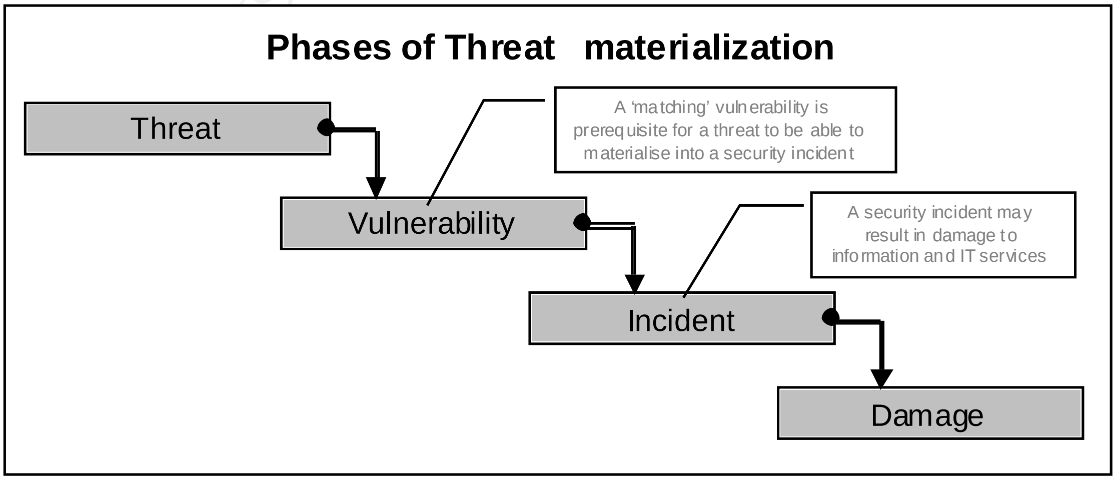
It should be obvious that as each of these elements generates costs and that each of them should be accounted for when implementing security measures.

Security measures

As there is no 'silver bullet' to security we will have to live with the fact that security measures mitigate only a part of all risks. Certain security measures may eliminate specific risks while others only reduce the risk. When implementing security measures it is important to be able to determine the residual risk.

In determining the remaining security risk it is very helpful to know in which phase of threat materialization (see picture) security measures are being deployed. This will also help in obtaining knowledge about the effectiveness of security measures implemented.

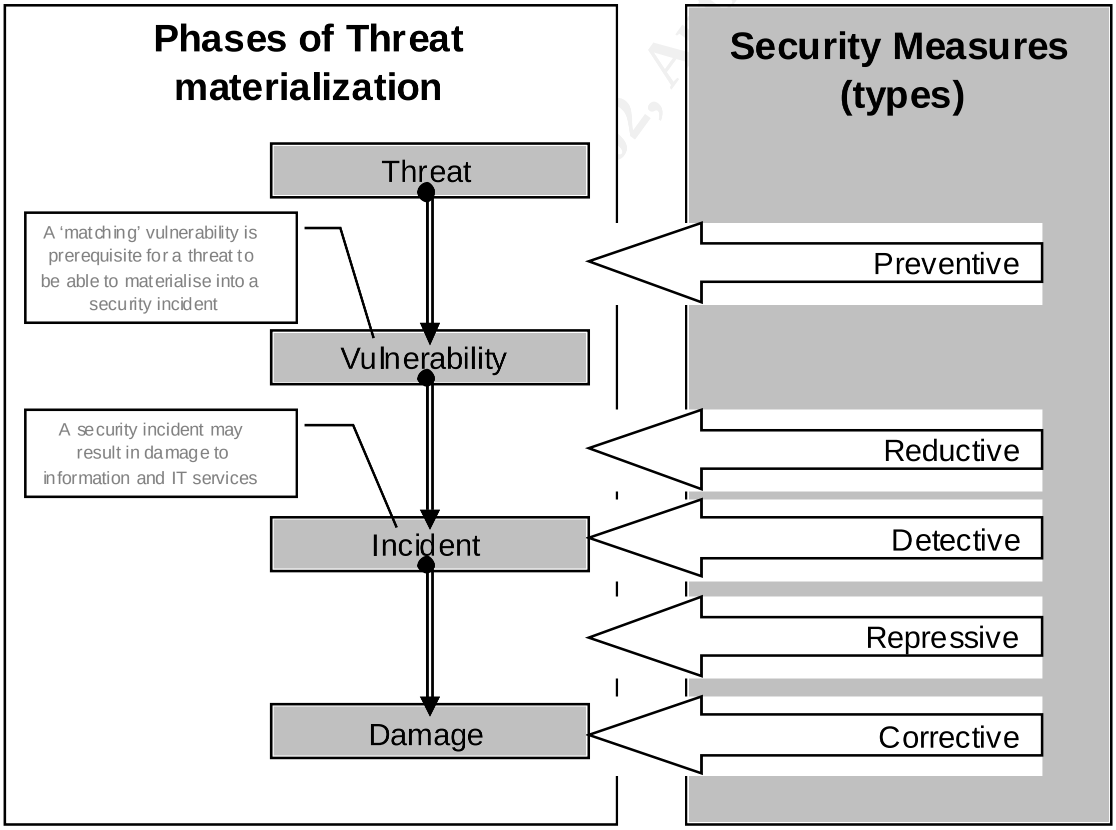
The picture below provides an overview of the phases in which a threat materializes into a security incident.


Phases of Threat materialization
Threat
Vulnerability
Incident
Damage
A 'matching' vulnerability is prerequisite for a threat to be able to materialise into a security incident
A security incident may result in damage to information and IT services

Phases of Threat materialization.

- <u>Threat</u>
  Security incidents depend on the existence of a threat. It should be known that security incidents are not purely caused by technical threats, the majority is a result of human (intended or not) and procedural errors.
- <u>Vulnerability</u>
  To cause a security incident a threat depends on the existence of a matching vulnerability. No vulnerability match no incident, it is as simple as that.
- <u>Incident</u>
  A security incident, depending on the business value of the information and IT services affected may result in more or less significant damage to that information or those services.
- <u>Damage</u>
  Damage to information and IT services of value to the Business has to be corrected.

The picture below provides an overview of the type of security measures that can be taken at each of the stages in which a threat materializes into a security incident.


Phases of Threat materialization
Threat
A 'matching' vulnerability is prerequisite for a threat to be able to materialise into a security incident
Vulnerability
A security incident may result in damage to information and IT services
Incident
Damage
Security Measures (types)
Preventive
Reductive
Detective
Repressive
Corrective

A description of the types of security measures:

- <u>Preventive measures</u>
  This type includes measures that can be taken before the incident takes place. They are aimed to prevent an incident from occurring and are focussed towards the

elimination of risks and/or vulnerabilities. Examples of this type are the secure configuration of Operating Systems, Firewalls and Vulnerability assessment.

- Reductive measures
  This type includes measures that also can be taken before the incident takes place. They are aimed at minimizing the damage in case an incident occurs. They are focussed towards the reduction of the impact of an incident. Examples of this type are the creation of regular backups and contingency plans.
- Detective measures
  This type includes measures that also can be taken before the incident takes place. They are aimed at detecting a security incident at an early as possible phase, preferably before causing any significant damage so that adequate repressive measures can be taken and the need for corrective measures is minimized. Examples of this type of security measures are intrusion detection systems and malicious code (e.g. virus) checking software.
  Note: this type is a special instance of a reductive measure because it is a prerequisite for the following two types of security measures. Without detection of the incident one wouldn't know when to take repressive or corrective measures.
- Repressive measures
  This type includes measures that also can be taken before the incident takes place, the actual execution of the measures takes however place after the incident occurred. This type of measures is aimed at minimizing the damage in case an incident occurs and are focussed to counteract the continuation or reoccurrence of an incident. Examples of this type are the automatic locking of user accounts after a specified number of unsuccessful log on attempts, the blocking of network addresses based on unauthorized access attempts and the creation and execution of security incident response measures such as Computer Incident Response Teams (CIRTs).
- Corrective measures
  This type includes measures that also can be taken before the incident takes place, the actual execution of the measures takes however place after the incident occurred. This type of measures is aimed at repairing damage and restoring the status to the original status before the incident occurred. Most measures take advantage of reductive security measures. Examples of this type are making use of fallback scenarios and the restoring of backups.

The information above underlines that security measures taken at the initial phase of threat materialization, i.e. preventive measures aimed at to elimination of risks and/or vulnerabilities tend to be the most efficient. One however should always take into account the costs of these measures and the necessity of multi-layered security.

Preventive security measures are likely to lessen the need for reductive, detective, repressive and corrective security measures. Keep in mind that I wrote lessen; this for the reason that also preventive measures are not the silver bullet to security ☹.

Be aware that the effectiveness and efficiency of the security measures must be evaluated to be able to determine whether the implemented measures meet the business need. Such an evaluation requires full reporting of security incidents and mitigated threats and vulnerabilities.

Business benefits of security measures.

By now it should be no surprise that security measures do cost money. On the other hand it should be obvious that security incidents resulting from not implementing security measures also do cost money. Organizations have to face the fact that they should make a balanced choice between budgeting for security measures and absorbing the cost of security incidents as a consequence of (taking the decision of) not implementing security measures. Making this balanced choice requires having accurate knowledge of the needs for security.

Security needs should be based on accurate knowledge of the risks an organization is exposed to, the impact of these risks in '$' and the costs of avoiding these risks. Without this knowledge there will be a tendency to either ignore significant risks or spend disproportionate amounts of money on minor risk mitigation. The fact that correction of an unbalance also requires the same knowledge even makes things worse.

Risks are reality but only controllable risks are acceptable

Having accurate knowledge of its needs enables an organization to document the security demands for IT. Knowing their security demands for IT facilitates the process of selecting the right security measures and/or security services.

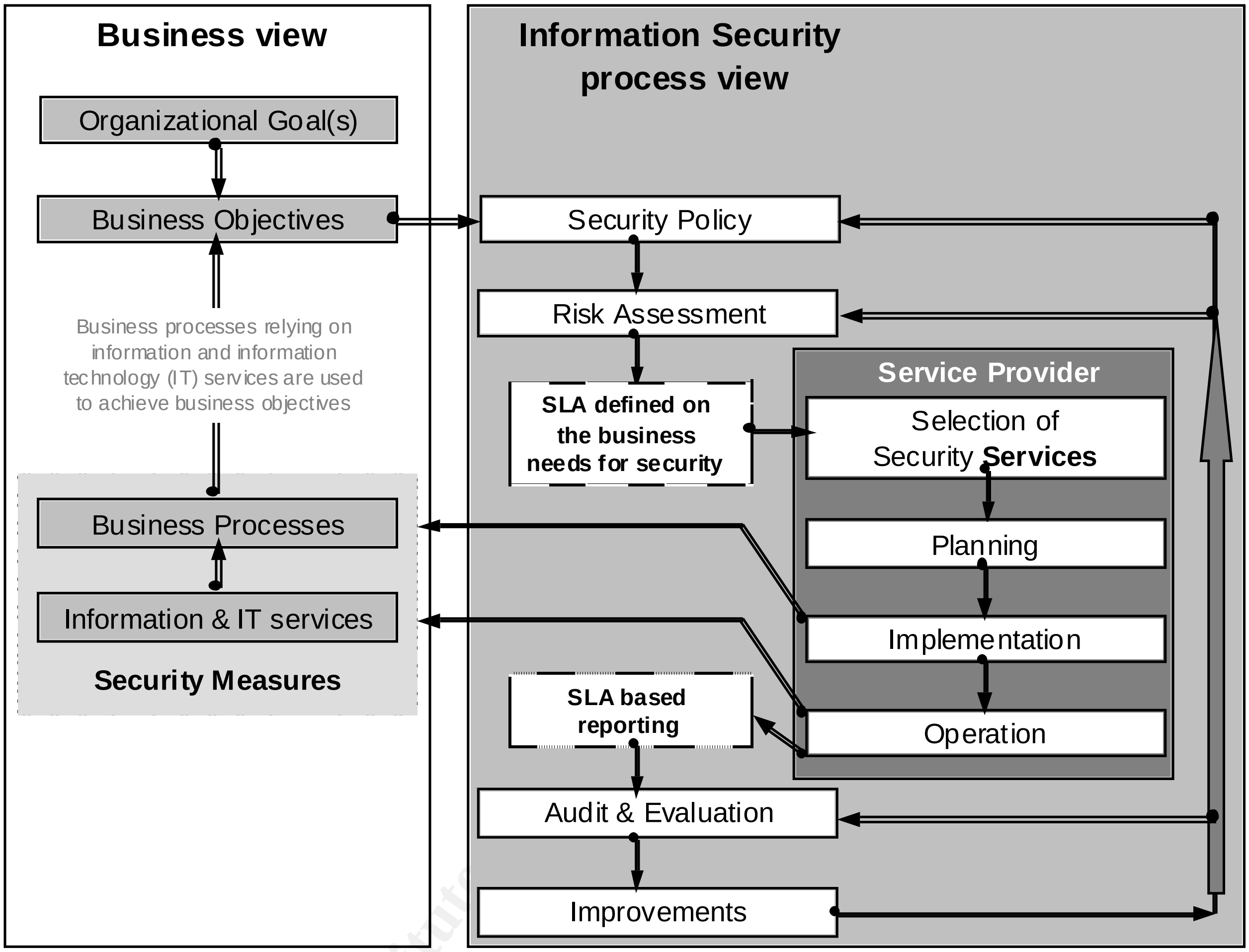
In particular when selecting security services organizations should use their documentation on the security demand for IT as the primary source of information. The same information should also be used as the requirement base when defining a Service Level Agreement (SLA) for security services with an IT service organization.

Organizations should be aware of the fact that an SLA provides the only mechanism that enables an organization to audit and evaluate the efficiency and effectiveness of security services provided by the IT service organization.

The picture shown at the next page attempts to visualize the SLA and SLA based reporting interfaces when a part of the security management process is subcontracted from an internal or external IT service organization.

The security needs, i.e. the security demand for IT stemming from the risk assessment is taken as a base for defining the SLA and thereby input for the selection of security services. To facilitate SLA based reporting the security needs should be defined in such a way that they are measurable.

Whether the security services delivered meets the actual business need can then be derived from information of the SLA based service reporting in the audit & evaluation process element.


Business view
Organizational Goal(s)
Business Objectives
Business processes relying on information and information technology (IT) services are used to achieve business objectives
Business Processes
Information & IT services
Security Measures
Information Security process view
Security Policy
Risk Assessment
SLA defined on the business needs for security
Service Provider
Selection of Security Services
Planning
Implementation
Operation
SLA based reporting
Audit & Evaluation
Improvements

What I do want reader to memorize is that the cost-effectiveness and so business benefits of security measures can only be measured and managed based on having accurate knowledge of the security needs and accurate feedback on the efficiency and effectiveness of security measures taken.

References:

1. [ITIL]
   Cazemier, Ing. Jacques A. Overbeek, Dr. Ir. Paul L. Peters, Drs. Louk M.C. Peters. IT Infrastructure Library - Security Management. London:The Stationary Office CCTA. ISBN 0 11 330014 X, 1999. 7-32.
2. [BS7799-1]
   BSI/DISC Committee BDD/2, Information security management. BS7799-1:1999 Information Security Management - Part 1: Code for practice of information security management. ISBN 0 580 28271 1, 1999.
3. [BS7799-2]
   BSI/DISC Committee BDD/2, Information security management. BS7799-2:1999 Information Security Management - Part 2: Specification for information security management systems. ISBN 0 580 28280 5, 1999.
4. [CobiT]
   COBIT Steering Committee and the IT Governance Institute ™. COBIT ® 3rd Edition - Framework. ISBN 1-893209-14-8, July 2000.
   URL: http://www.isaca.org/ct_frame.htm (6 June 2001)
1. [OCTAVE]
   Alberts, Christopher. Dorofee, Audrey. OCTAVE SM* Threat Profiles. Publication date unknown.
   URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf (6 June 2001)
2. [RMG]
   NIST National Institute for Standards and Technologies. Risk Management Guide. Special Publication 800-30. 1st Public exposure DRAFT - June 2001
   URL: http://csrc.nist.gov/publications/drafts/riskmgmt-guide-draft.pdf (6 June 2001)