**Risk Management, or a Global View of Enterprise Security**

GSEC Practical Assignment 1.4b Version 1.1

Klaus Hornung
8 April 2003

**Table of Contents**

## 1. Introduction

Today, security is becoming a matter of growing importance for every modern company. The dissemination of the Internet and the growing acceptance of e-business, e-commerce and e-retailing render appropriate security measures indispensable within the company. Never before has security been attributed such great importance as a way of ensuring corporate survival, of achieving a decisive competitive advantage and of sustaining stakeholder value. For this reason, an effective security program needs to provide more than just equipment and technology – it also needs to integrate people and work flows within the company.

This document tries to point out all relevant steps for successful risk management. Because of the complexity of this subject it can be a rough description only. One important point to focus on is the notion of security policy. As the importance of security policies that are relevant for enterprise security are often underestimated, part of this paper will deal with this topic.

## 2. "History" of Risk Management

The major challenge facing many companies today is posed by global communication with distributed systems, mobile availability, and all this in real time. On the other hand, there is a desire for availability, confidentiality and integrity. Historically, the security strategies adopted to this end have changed over time. In the eighties the main concern was the provision of physical protection. Gates and fences were erected around the company, guards monitored access, and data were protected physically in fire-proof rooms. All measures to protect the company against external threats.
The motto of the nineties was "find and repair." Internal and external electronic threats were analyzed in order to identify attacks against confidentiality, availability and integrity. These were mainly reactive measures aimed at identifying and documenting incidents and attacks. This was the era of classic Intrusion Detection Systems, be they network and/or computer-based.
Today, the main emphasis should be placed on security management, i.e. on risk analysis and the drafting and implementation of security policies. A company's image and the trust of its employee, partners and customers are at stake. Financial viability and business success are at risk. In the foreseeable future companies will have to tackle the following important aspects:

- Network performance. How can one protect the company's network infrastructure against internal and external attacks, for example denial-of-service attacks or floods of unwanted advertising mail?
- Responsibility. How can one protect the company against legal action, which may arise because of inappropriate or unlawful use of Internet resources?
- The loss of internal information. How can one assure that valuable company secrets and sensitive information do not fall into the wrong hands?
- Financial losses: how can one prevent the impairment of productivity due to the abusive wasting of time and resources and down-times caused by crashes. How can one support the administration of system resources?

- Reputation: how can one avoid the loss of credibility and image caused by insecure computer systems, malfunctions, the violation of customers' privacy and slow communication?

## 3. What constitutes a risk for a company?

A risk is a future event the result of which is a failure to implement corporate objectives. Different risk classes need to be borne in mind such as, for example, the financial, market, management, image, environmental and IT risks. Here, we take a closer look at the IT environment risk, which we represent using the following formula:

***IT RISK = potential threat X weak points X amount of damage***

In order to minimize risk an attempt must be made to reduce one or several of these three factors (potential threat, weak points, amount of damage). It soon becomes clear that little can be done to change the potential threat and that this must, unfortunately, be regarded as a fixed parameter. The company is hardly in a position to reduce the scope of illegal and criminal acts in the Internet. It can at best exert limited influence on the potential threat within the company. To this extent, the potential threat must be recognized as a fixed parameter.
The amount of damage, in other words the value of the information that is to be protected, is also static. Reducing this value would be tantamount to abandoning the company's targets. The task of Risk Management is to determine the value of this information.
The identification and evaluation of all weak points within the company constitute the third factor that needs to be addressed.
Once the risk has been identified, various approaches may be adopted:

1. The full risk is borne.
2. An attempt is made to avoid the entire risk by reducing one of the three parameters to zero
3. The risk is minimized.

It is obvious that the only meaningful way to minimize risk is to reduce the weak points. This approach is also supported by the fact that 95% of all security events reported to the CERT could have been prevented by rectifying weak points in good time (http://www.cert.org/present/cert-overview-trends/module-2.pdf). This makes it possible to achieve the objective of keeping the risk exposure within a target corridor agreed on in the company's security policy.

## 4. The four phases of risk management

Risk management for IT security is today made up of several different phases: assessment, planning, implementation and monitoring. This new, comprehensive method has been developed in order to be able to produce analyses that are important for the enterprise's management and for elaborating appropriate recommendations that can be incorporated in a company's overall corporate policy, its objectives and business targets.

## 4.1. Assessment

During the assessment phase all weak points are identified. There is no standard risk-assessment model. Some companies rely heavily on methodology and calculations, others on the more qualitative question-and-answer method. All assessment models need to take account of uncertainties. The procedure to be followed within the framework of risk assessment is as follows:

### 4.1.1. Fix a target.

Before the assessment starts CIOs or IT managers should determine the reasons for implementing a risk management system. A large number of companies regard risk management as part of their corporate policy. If, for example, a company puts after-sales service right at the top of its list of priorities, then the main objective for risk management could be to avoid those threats that could lead to these services being interrupted. Although these targets may differ from company to company, risk management fulfils the same main task for all: it should have a positive impact on the entire company.

### 4.1.2. Prepare an inventory of all systems/resources that are critical for the company.

All resources that are to be protected should be listed individually (including data and contents relevant to the company, passwords, services etc.). The inventory that is drawn up should include all systems, services and components.

### 4.1.3. Emphasize the threats clearly.

Identify briefly which persons or events could damage corporate resources. Examples here are hackers, viruses, discontented employees, human error or system failure.

### 4.1.4. Identify the weak points.

In order to identify possible threats to the company's resources a method should be used that has no negative repercussions and does not cause interruptions. Explicit attention should be drawn to areas that are particularly risk-prone. Potential weak points include network access points, existing applications and servers. In extensive distribution chain networks that are used by suppliers the number of access points increases, which also makes the network more vulnerable.

### 4.1.5. Measure the risks from the financial point of view.

As it is impossible to prevent all threats completely, IT departments have to focus on the most crucial resources and weak points. IT managers can more easily determine the priority of individual security measures and expenditure if network risks that threaten the company as a whole are first analyzed numerically.

## 4.2. Planning

The planning phase builds on the assessment phase. This phase lays down security policies for security measures. These policies are based on the corresponding repercussions on certain risks as well as on the achievement of general business objectives. The success of planning in risk management depends on two factors: acceptance among senior managers and effective, inter-departmental communication.

### 4.2.1. Prepare a security policy.

Without clear security guidelines even the most efficient security solutions are ineffective. Such guidelines lay down how, why, when and by whom security measures are to be taken.

### 4.2.2. Definition of a security policy

A security policy consists of assumptions, rules and principles stipulating how information security is to be implemented in the company.
It accordingly provides the framework ("bible") within which information security operates.

### 4.2.3. The bases of a security policy

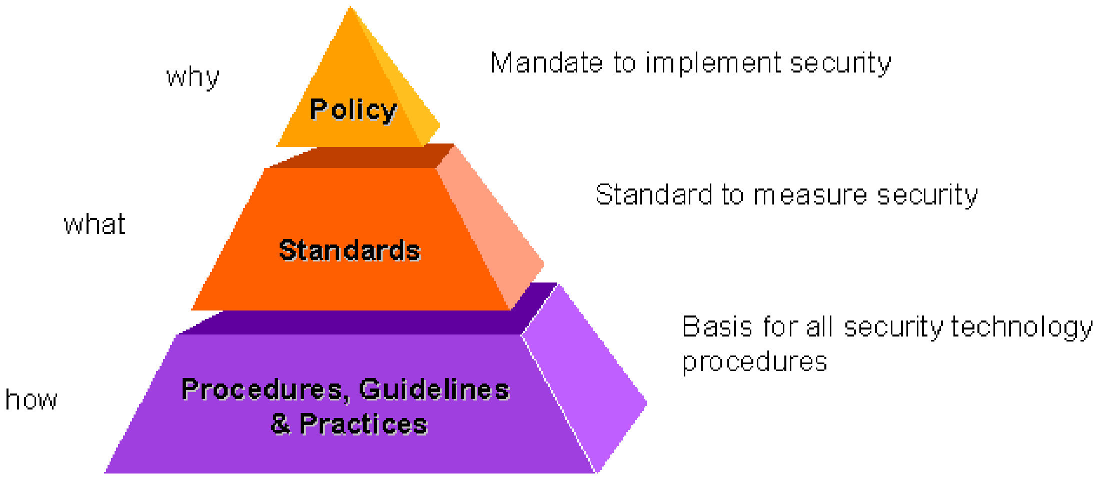
A security policy always depends on the security requirements of the individual company and naturally does not of itself alone signify security. Only the implementation of and compliance with these rules brings the desired security, i.e. a security policy "lives" and has to be monitored and trained continuously. The preparation and continuation of the security policy must be an integral part of the company's business processes and is thus a matter for senior management. In addition, the necessary investment for the drafting and implementation of such a security policy must be budgeted for and made available in good time.

### 4.2.4. Basic rules of a security policy, it must

- have a clear objective,
- be seen to be issued by the management/board,
- be clear, comprehensible, unambiguous and free of contradictions (keep it simple),
- be clearly structured and organized (basic policy, sub-policy,...),
- use motivating and explanatory formulations (strict prohibitions should be avoided),
- be auditable and transparent.

### 4.2.5. The structure of a security policy

Building a Security Policy


why
Policy
Mandate to implement security
what
Standards
Standard to measure security
how
Procedures, Guidelines & Practices
Basis for all security technology procedures

A three-stage concept provides a very good structure for the preparation of a security policy. The board's mandate to initiate this process should come first here. This must be clearly recognizable as such and must be made public. This mandate, which is often referred to itself as a policy, defines WHY this policy is to be created and implemented. In addition, the Chief Executive Officer (CEO) as information owner should be clearly identifiable as the person responsible for this policy.
The second step is to authorize the Chief Security Officer (CSO) to prepare and implement the policy. The CSO defines the level of security the company needs. This may take the form of standards created by the CSO himself or may be based on existing standards, e.g. ISO 17799.
These documents contain detailed descriptions on the areas that should be taken into account in the weak-point analysis. The ISO standard supports companies in developing a security policy and is implemented in a large number of countries. The documents can be obtained in Chinese, Danish, Dutch, Finish, French, German, Japanese, Korean, Norwegian, Portuguese, Spanish, Swedish and English. Companies can then also use the ISO standard as guidelines for developing a qualified information-security program if they are not aiming for certification.

The areas covered by the ISO standard include:
(http://www.iso17799software.com/what.htm)

- Business Continuity Planning
- System Access Control
- System Development and Maintenance

- Physical and Environmental Security
- Compliance
- Personnel Security
- Security Organisation
- Computer & Operations Management
- Asset Classification and Control
- Security Policy

The level of security required for each company differs greatly and can only be determined by way of a risk analysis.

The second stage identifies WHAT precisely is to be implemented.

The third stage then consists of breaking down the defined standard at the implementation level. Precise instructions are defined here as to how this standard is to be implemented in practice. For reasons of technical feasibility this must be done in close co-operation with the Chief Information Officer (CIO).
Based on this structure it is then also possible to lay down the various areas of responsibility:

**Tasks of the decision makers (responsibility and design von security)**

- What areas are covered by IT security?
- Assessment of the current situation.
- Determination of the value to be secured (not least for insurance purposes).
- Determination of the security requirement and priorities.
- Define standard.
- Define and implement guidelines and processes.
- Product selection.
- Recruitment of human resources and training.
- Budget.

**Tasks of the administrators (implementation and realization)**

- The policy.
- Discovery of security gaps.
- Analysis of log files.
- Advanced training in all sectors of IT security.
- Keeping abreast of changed security requirements.
- 7X24 hours of monitoring.
- Implementation of daily business operations (customer and employee support).

### 4.2.6. Elaborate a security monitoring procedure.

Regular checks keep IT managers and managers from other divisions informed of the efficacy of the security strategy. However, before the IT department can run checks managers must lay down a procedure for answering the following questions. Who will carry out the checks?

Should the measures be carried out in-house? Or should outsourcing be considered? What methods are used to analyze security data? Who should check the data? Who should determine whether it is necessary to modify the security system?

### 4.2.7. Define effective technical procedures.

Several “what happens if” questions relating to potential risk scenarios in the technology sector should be posed and answered by the IT department.

- **With respect to security violations:**
  Define how the IT department and users should behave in the event of hacker attacks, viruses or other security violations. Whom should users inform if they find a virus? Under what circumstances would the IT department close down the company’s e-mail server or network? What method of communication is used by the IT department to inform users of warnings and emergencies?
- **With respect to modifications to the network and server configuration:**
  Identify a person who is responsible for modifications to the network and server configuration. Define why and when this person should make such modifications.
- **With respect to the introduction of new applications:**
  Is there a test procedure that can be used before new applications are introduced? Who is responsible for data conversion? What steps have to be taken into account by users when introducing new applications?

### 4.2.8. Appoint a reaction team and prepare a disaster recovery plan .

Members of the reaction team are allocated areas of responsibility for emergencies. Appoint a team leader for this reaction team and set guidelines for the relevant deployment procedures.
Drafting a watertight disaster recovery plan is an art in itself. A disaster recovery plan is a decisive component of every risk-management solution. disaster recovery plans spanning entire networks deal with top-level problems such as, for example, server backups, the deployment of additional human resources, specialist personnel, dealer services and relationships.

## 4.3. Implementation

All the measures mentioned so far, particularly the Security Policy, merely constitute a set of theoretical rules, a “mental summary.” Naturally, these rules alone do not create security, only their implementation brings the desired protection.
The task of IT managers is to provide network security products such as firewalls, anti-virus, e-mail and Internet-content filtering software that are appropriate to the network requirements. Not all applications are appropriate for all networks. IT managers’ selection of security applications that are appropriate to the specific security requirements of the company and of the

end-users should be based on the findings of the risk-management analysis. To this end, IT managers must cooperate with heads of department or the personnel department in order to identify what level of security is to be allocated to individual users. A member of the IT team should be allocated the task of configuring different applications security levels. It also makes good sense for the IT department and management to draft a guideline on the allocation of individual, user-dependent security rights.

## 4.4. Monitoring

Risk management is an ongoing process that is not brought to an end by the introduction of a security system. Regular monitoring of the IT environment allows IT employees to identify which security applications are effective, for which areas stricter security measures need to be imposed and how changes in the company impact security in general.
These data, which are identified by a policy compliance tool, provide the basis for risk management from the strategic point of view. From the point of view of day-to-day business operations, administrators and security officers are alerted to attempted security violations by the use of monitoring tools. The range of such monitoring tools includes:

### 4.4.1. Policy Compliance Monitoring

Policy Compliance Monitoring tools which monitor compliance with the security policy in important e-business applications and operating systems throughout the entire company. Intelligent tools allow administrators to create a security strategy for each system rapidly and cost-effectively and to monitor and measure its compliance. Systems that do not comply which the security guidelines should be identified fast. In this way incorrect settings can be corrected in a timely manner in order to guarantee compliance with the security policy. The greatest attention should be attached to the monitoring of the security policy. The detection and prevention of all weak points in the IT environment brings the greatest gain in security. All other solutions should be based on this. The situation today is, that the amount of vulnerabilities are increasing. CERT reported in 1995 171 vulnerabilities only, in 2002 the amount of vulnerabilities raised up to 4,129 (http://www.cert.org/stats/). There is no way anymore to handle all weak points in an enterprise environment by “hand”. This situation demonstrate the need of a Compliance Tool for that area.

### 4.4.2. Example of a Policy Compliance Monitoring Tool

Symantec Enterprise Security Manager provides security policy compliance management of mission critical e-Business applications and operating systems across the enterprise. From a single location, it manages the discovery of policy deviations and vulnerabilities for services housing mission-critical applications and data on the network, enterprise wide. With its intelligent tools, administrators can create baselines and measure performance against those baselines to identify systems that are not in compliance and correct faulty settings to bring systems back into compliance.

(http://enterprisesecurity.symantec.com/products/products.cfm?productid=45&EID=0)
In this example two sets of Policies (Login Parameter, Password Strength) where monitored against a default Microsoft Windows 2000 Workstation:

### Login Parameter:

| Check Name | Long Description | Result | Description |
|---|---|---|---|
| Account Lockout Enabled | This check verifies that account lockout is enabled and set to lock out an account after a specified number of bad logon attempts. | ✖ | Account lockout is disabled: The account lockout function is disabled. Accounts will not be locked out after a specified number of bad logon attempts. User accounts are exposed to brute force logon attacks. |
| Lockout Time | This check reports a problem if the account lockout time setting is less than the time specified in your policy. Set the policy value to zero if accounts should be locked out until reset by the administrator. | O.K. | |
| Time Before Bad Logon Counter Is Reset | This check reports a problem when the bad logon lockout counter can be reset to zero before the time specified in your policy has elapsed. | O.K. | |
| Display Legal Notice During Logon | This option ensures a user defined legal access notice is displayed before users logon the system. The notice provides legal protection against unauthorized users. If a notice is defined, it will be displayed in the ESM report. | ⚠ | No legal notice defined: Your system does not display a legal access notice before users log on. Legal notices increase the legal liability of unauthorized users who access the system. Define the message text and title for this notice in your Windows 2000 security policy. |
| Hide Last User ID from Logon Dialog Box | This option checks that the last input user ID is not displayed in the logon dialog box. This protects the user ID from unauthorized use. | ⚠ | Last user ID is not hidden: The user ID of the most recently accessed account appears in the Logon dialog box. This gives away half the User ID / Password combination intended to protect the account from unauthorized access. You should hide the previous user ID by setting the following registry entry to 1: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ policies \ system \ dontdisplaylastusername. |
| Do Not Allow Shutdown from Logon Dialog Box | This option checks that the shutdown button is disabled in the logon dialog box. This is done to prevent unauthorized users from shutting down the system. | ⚠ | Shutdown from Logon dialog box is enabled: Users can shutdown the system without logging on first. This lets anyone interrupt system operations. You should disable this function if the system is secure from power interruptions. This is done by setting the following registry entry to 0: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ policies \ system \ shutdownwithoutlogon. |

### Password Strength:

| Check Name | Value | Long Description | Result | Descriptions |
|---|---|---|---|---|
| Minimum Password Length | 8 | This check reports a problem if the Windows 2000 Password Policy allows passwords to be shorter than the specified number of characters. | O.K. | |
| Accounts Without Passwords | | This check reports user accounts that can be accessed without entering a password. The user list lets you exclude user accounts that should be excepted from the check. | ✖ | . No password: The accounts listed below do not have passwords. This is a security problem because anyone with the user name can access these accounts. You should immediately assign passwords to these accounts. Instruct each user to log on using the assigned password and then to change the password again. |
| Password = Username | | This check reports a guessed password when the user name and password are identical. The check is provided for systems with a large | O.K. | |

| | | | | |
|---|---|---|---|---|
| | | number of user accounts. The check is not as thorough as "Password = Any Username." However, if the "Password = Any Username" check takes too much time or consumes too much CPU, you can use the "Password = Username" check on a daily basis and the "Password = Any Username" check on the weekends. | | |
| Password = Any Username | | This check examines each password for a match with any user name. | O.K. | |
| Password Must Expire | | This check reports a problem if passwords do not expire on the Agent system. If the system does expire passwords, the check reports user accounts that have enabled the user properties setting, "Password Never Expires." By default, this check does not report users who cannot change their passwords. If you want the check to report users who cannot change their passwords, enter Yes in the "Yes or No" text box. Use the name list to exclude users and security groups from the check. | O.K. | |
| Maximum Password Age | 60 | This check verifies that the Windows 2000 Password Policy has a maximum password age, which does not exceed the number of days specified in your security policy. | ⚠ | Minimum password age too low: The minimum password age is set too low. Users have trouble remembering passwords that change too often. Users may cause security breaches by writing down passwords instead of memorizing them. The recommended minimum password age is 14 days. |
| Minimum Password Age | 14 | This check verifies that the Windows 2000 Password Policy has a minimum password age and that a password cannot be changed before the specified number of days has elapsed since the previous password change. | O.K. | |
| Password Uniqueness | 10 | This check verifies that the Windows 2000 Password Policy requires a specified number of passwords to be retained as password history. These passwords cannot be reused when a password is changed. | ⚠ | Minimum password history too low: The number of passwords required to be retained as password history is set too low. This lets users recycle expired passwords too quickly and defeats the requirement to change passwords on a regular basis. A password history setting of at least 10 is |
| Check for Syskey Encryption | | This check verifies that syskey encryption is enabled. | O.K. | |

**4.4.3. Intrusion Detection Software** which monitors either networks or hosts for suspicious traffic. non-disruptive intrusion detection solutions are able to differentiate between "normal" traffic and conspicuous data packages, warn system managers and terminate a connection in the event of abnormal activity. These solutions also generate network traffic log reports.

**4.4.4. Firewalls** offer back-end network protection against intruders attempting to penetrate the system. Most applications warn IT managers if an attempt has been made to gain unauthorized access and generate log files on such attempts.

**4.4.5. Virus shield** programs monitor a system for potential viruses and repair them or place them in quarantine. Most virus-shield software draws IT managers' attention to suspicious viruses.

#### 4.4.6. Security violations:

**Internal:** e-mail content filtering can monitor incoming and outgoing messages for confidential or libelous material. Internet content filtering can prevent users calling up websites with unsuitable or possibly damaging contents. Both methods generate log reports for the IT department on user activities and violations of guidelines.
**External:** authentication and encryption software protects the network and the data to be transmitted against intruders by requiring passwords or private encryption codes before allowing access to data. These security tools are often able to generate reports on unauthorized access attempts.

## 5. Integrated risk management

Ideally, risk management should be an important component of a company's day-to-day operations. New, automated tools make it easier to integrate risk management solutions throughout an enterprise in that security analyses are passed on into recommendations that have a positive impact on the entire company. Senior management is increasingly mandating the IT department not only with the task of looking after security measures, but also of elaborating the guidelines and procedures associated with them. A thorough and well-thought-out approach to risk management provides the IT department with a solid foundation on which to base its security principles.

## 6. References:

International Standards Organization
http://www.iso.org/iso/en/ISOOnline.frontpage

ISO 17799: What Is It?
http://www.iso17799software.com/what.htm

CERT/CC Statistics 1988-2002
http://www.cert.org/stats/

CERT/CC Overview, Incident and Vulnerability Trends
http://www.cert.org/present/cert-overview-trends/module-2.pdf

Symantec Corporation
http://enterprisesecurity.symantec.com/products/products.cfm?productid=45&EID=0