May 2009

Investigating Insider Threats: Problems and Solutions

Master thesis

Business Administration, Information Management
University of Twente

(public version)

W. Cornelissen

Investigating Insider Threats: Problems and Solutions

Master thesis
Business Administration, Information Management

Date	: May 6, 2009
Author	: **W. (Wesley) Cornelissen MSc**
Email	: mail@wesleycornelissen.nl
Studentnumber	: s0044067
Institute	: University of Twente, Enschede (Netherlands)
Faculty	: School of Management and Governance (SMG)

Graduation Committee

Supervisor	: **Dr. Ir. A.A.M. (Ton) Spil**
Institution	: University of Twente, Enschede (Netherlands)
Faculty	: School of Management and Governance (SMG), Information Systems and Change Management.
Supervisor	: **Ir. V. (Virginia) Nunes Leal Franqueira**
Institution	: University of Twente, Enschede (Netherlands)
Faculty	: Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS), Information Systems Group

Management Summary

Research motive

This master thesis was motivated by a question from a chemical company that was aware of the need to safeguard confidential information against potential threats that could be posed by trusted insiders (i.e. employees, business partners, visitors). Based on the question that rose, ‘*what can we do to protect our valuable information against misuse of trusted insiders?*’, research has been done on the actual risk of insider threats and measures that could be applied to mitigate these risks.

Conclusions

Based on an extensive literature review it can be concluded that:

- The scientific literature on the insider threat problem is not yet mature. There is a lack of appropriate definitions and contextual information, but also data for analysis, experimentation and, ultimately, validation of proposed solutions.

The multiple case studies showed that:

- Insight in, for example, the effectiveness of measures is, however, also lacking at the case study organizations. In practice more attention is given to the implementation of measures, without knowing the actual threats that need to be mitigated. Deliberate misuse by insiders is considered negligible and is accounted for as a residual risk.

Recommendations

To address and mitigate insider threats, firms are recommended to:

- Apply a risk assessment and analysis to gain insight in the possible threats and vulnerabilities to which the organization is exposed.
- Determine a corporate risk minimization strategy for each of the identified risks (i.e. risk acceptance or risk reduction).
- Select formal, informal and technical security measures that address the identified threats and vulnerabilities, in accordance with the risk minimization strategy.
- Create commitment and awareness of both management and end-users, through the application of security education, to gain support for the implementation of selected measures.

Motivation

An extensive literature review resulted in insight in the insider threat problem. Based on the literature review, it was clear what characteristics insiders had in common, what the causes of insider threats were and what the potential risk of insider threats was. In addition, the literature review resulted in a list of mitigating measures. The application of these measures in practice was evaluated through a multiple case study that included a cross-section of organizations. The case studies not only showed that risk assessments are not the point of departure for the application of security measures in practice, but also that there is a gap between the measures that were found in literature and the measures that are applied in practice.

Consequences

There are of course costs and efforts related to the application of security measures. These costs and efforts include not only financial expenditures on IT resources, but also reductions of productivity and creativity, and an erosion of trust between employer and employees. The importance of selecting appropriate measures is to balance between these costs and the level of security that result from having the measure.

Table of contents

List of figures

List of tables

Foreword

In front of you lies my master thesis, which finalizes my Master of Science degree in Business Administration at the University of Twente. This master thesis is the result of an extensive literature review and multiple case studies I conducted in the period between October 2008 and May 2009.

This master thesis started in fact with a question that my manager asked me, early 2008, when I was working part time at a chemical company. Since my first internship, in 2005, I worked there on different tasks that all related in some way to information security. This question showed, however, a completely different perspective of the topic of information security: “What can we do to protect our valuable information against misuse of our own employees?”.

In July 2008 I started to think on how to address this question, being the point of departure for my master thesis. At that time I followed a course of Daniel Moody, who suggested conducting a literature review and multiple case studies. These multiple case studies would give an impression on how firms address the problem of insider misuse in practice. From that time on, I started searching for firms that were interested in the topic of my research. This, however, proved to be hard. Firms were interested in the topic, but were not willing to share information on their information security efforts, due to the sensitivity of the topic. It is therefore that in this foreword, and throughout this master thesis, the case study organizations and persons involved were made anonymous.

In October 2008 I started working on my master thesis, and soon after the start I found two additional cases that were willing to cooperate: a public institution and a care institute. After an extensive literature review and some interviews I started writing on this thesis. All this, however, has not been just my work. Ton Spil, Virginia Nunes Leal Franqueira and my manager at the chemical company were the ones that helped me to stay on track. They shared their thoughts and opinions with the goal of improving the overall quality of this document. I would like to thank them for their patience, remarks and efforts.

Several others have also spent their time and thoughts on this project; sometimes after I asked for their opinion, sometimes spontaneously, but always valuable. I would especially want to thank the interviewees at the public institution, care institute and chemical company that were willing to answer my sensitive questions. After three years of working part time at the chemical company, finishing this master thesis means also saying goodbye to a group of people which were always interested in both my study and personal life. I would, therefore, like to thank my colleagues for the time and moments we shared together.

There are, of course, many more people to thank, who all influenced this work. This group includes my parents, who always supported me to attain my goals, and my girlfriend and friends, with who I shared my ideas, wishes and frustrations. I am proud of the result and I hope you will enjoy reading it.

Wesley Cornelissen,

Arnhem, May 2009

1. Introduction

This master thesis started with a question from a chemical company in the Netherlands that operates in a highly competitive market. The company uses a patented process to produce goods that are applied in a variety of end-products. Because of the intellectual property and specific knowledge that is available to insiders (i.e. employees, business partners, visitors), the question rose on "How to protect intellectual property and other valuable information against misuse of these insiders?".

Like the chemical company, many other modern organizations make use of a sheer amount of information and information systems. Organizations that value their information, need to safeguard it from threat agents that exploit vulnerabilities in information systems and/or information security measures. Although attacks originating from outside threat agents, such as hacking attempts or viruses, have gained a lot of publicity, the more risky attacks come from inside (Schultz, 2002; Baker et al., 2008). Insiders are trusted and, therefore, have the necessary access to be able to exploit vulnerabilities more easily.

There are plenty examples of firms that experienced the results of insider attacks. An executive's administrative assistant at Coca Cola Co., for example, was recently accused of going through files and stuffing her personal bag with a sample of a new Coca Cola product and corporate documents. Her intention, along with two other people, was to sell this information to Pepsi Co. for 1.5 million dollars (Carroll, 2006). Another case which has gained a lot of publicity was the case of Nick Leeson who caused the collapse of the Barings Bank, the United Kingdom's oldest investment bank. Leeson had gained an immense amount of trust through his profits and was therefore able to circumvent many of the security inquiries against him without consequence. In this manner Leeson was able to hide his losses, eventually reaching £827 million, in a secretly created account using Barings' accounting computer systems (Dhillon, 2001). However, not all insider threats are posed deliberately. A company cofounder of Banner Therapy, a company that sells massage equipments, removed a hard drive from her work computer and had taken it home over the weekend to prepare for a client meeting. The hard drive contained all company records from the past seven years and Banner Therapy was basically out of business without the hard drive (Predd et al., 2008).

The threat posed by insiders is, however, not new. In 1978 already, Donn Parker estimated in his book "Crime by Computer" that 95% of computer attacks were committed by authorized users of the system. It should be noted however that this was in the pre-Internet era, when very few non-insiders had any access at all; still, the underlying issue – that employees are not always trustable – remains. To be sure, this has always been true – thieving or otherwise corrupt workers have undoubtedly existed since commerce itself – but the power of computers (and the inability to secure them in the best of circumstances) makes the problem far worse today (Bellovin, 2008).

Surveys confirm this and reveal that current or former employees are the second greatest cyber-security threat, exceeded only by hackers (Greitzer et al., 2008). In addition, these surveys reveal that the number of security incidents has increased geometrically in recent years. Due to the perceived risk of bad publicity and the fact that insiders could easily go undetected the reported number of security incidents caused by insiders could in fact even be higher. In addition, surveys reveal that the impact of security incidents is far greater than those caused by outsiders (Baker et al., 2008; Vadera et al., 2008). Organizations can suffer from direct effects, such as financial losses (Furnell and Phyo, 2003) or compromised records (Baker et al., 2008), but also from indirect effects. These indirect effects include, for example: risks to reputation that could dramatically impact stock prices, or losing competitive advantage, due to loss of intellectual property (Sinclair and Smith, 2008).

Despite the likelihood of insider attacks and the potential magnitude of their impact, companies are still not doing enough to protect themselves against this kind of threat (Melara et al., 2003).

In a recent literature review researchers concluded that the number of information security research papers published in the leading IS Journals has diminished (Siponen & Willison, 2007). The few models of and studies about insider attacks and related issues that are available in scientific literature are a good start, but they are of little value in producing meaningful results that can help organizations reduce the frequency of and damage from insider attacks (Schultz, 2002). There is a lack of appropriate definitions and contextual information, data for analysis, experimentation and, ultimately, validation of proposed solutions. This lack of data is driven by a variety of factors, the most prominent of which appears to be the sensitivity of the topic: organizations that have been the victims of insider attacks tend to handle such (known) incidents as quietly as possible (Keromytis, 2008).

Based on the likelihood of insider attacks and their potential impact, the question of the chemical company seems to be justifiable. Despite its importance, the insider threat problem is, however, not properly addressed in both theory and general practice.

1.1. Research problem

The importance and complexity of addressing the insider threat problem have resulted in the formulation of the following research problem for this master thesis:

What can firms, the chemical company in particular, do to protect their information against the insider threat problem?

1.2. Research objectives

The objective of this master thesis is to provide information security professionals, as well as responsible management, with an in-depth understanding of the characteristics of insiders, the possible threats insiders can pose, the potential risk of insider threats and the possible measures that can be implemented to address them. This understanding is based on both literature review and multiple case studies. By providing this in-depth insight, the master thesis will contribute to IS Security research.

For the chemical company this understanding of the insider threat problem results in an identification of the insider threats to which information is possibly exposed and an advice, including selection and prioritization of measures, aimed at their specific situation. The selection and prioritization of measures is based on both the strengths and weaknesses of these measures, derived from the literature review and multiple case studies.

1.3. Research questions

The three research questions below support the research problem and objective by acquiring knowledge from both scientific literature and multiple case studies. The scientific literature gives insight in the characteristics of the insider threat and possible solutions or mitigating measures to address the insider threat. The multiple case studies give insight in the occurrence of the insider threat problem in practice, the specific measures that are taken to counter or mitigate this threat and the strengths and weaknesses of these measures in practice.

I. What is the insider threat problem?

To be able to understand, define and describe the insider threat problem, answers to the following sub-questions are acquired by conducting a thorough literature study:

- Who can be defined as an insider?
- What are the root causes of the insider threat problem?
- What kind of threats can be perpetrated by insiders?
- How serious is the problem of the insider threat?
- What elements of the insider threat problem make it so hard to deal with?
- How can the insider threat problem influence the confidentiality, integrity and availability of information?
- What kind of information is subject to threats from insiders?

II. What possible solutions and mitigating measures, both theoretical and practical, exist to address the insider threat problem?

To acquire knowledge about the possible solutions and mitigating measures to address the insider threat problem a literature review and multiple case studies are conducted. The literature review analyzes possible measures from a theoretical viewpoint, the multiple case studies show what kind of solutions and mitigating measures are actually used by firms in practice.

Theoretical research questions:

- Which formal, informal or technical mitigating measures are available to address the insider threat problem?
  - Which mitigating measures are available to predict and detect insider threats?
  - What mitigating measures can be applied to respond to the occurrence of an insider threat problem?

Practical research questions:

- Which formal, informal or technical mitigating measures are used to address the insider threat problem?
  - Which mitigating measures are used to predict and detect insider threats?
  - What mitigating measures are applied to respond to the occurrence of an insider threat problem?

III. What are the strengths and weaknesses of mitigating measures in addressing the insider threat problem?

Answering this research question attains more insight in the decisions that should be made in applying the available mitigating measures in a business environment. Additionally, it aims at determining drawbacks of the measures used in practice and what measures could have been used according to literature review. Multiple case studies, complemented by a literature review answer this research question. The sub-questions that are addressed are:

- What are the trade-offs involved with the mitigating measures which address the insider threat problem?
- What determines the choice for one mitigating measure rather than another?

1.4. Scope

The scope of this master thesis is determined as follows:

This master thesis describes only threats that are posed by insiders

Threats can be posed by different threat agents. Threats can be caused by nature, the environment and by humans. This master thesis only focuses on threats caused by humans and solely to those humans that can be considered insiders (section 3.1.2).

This master thesis describes insider threats to both physical- and digital information

The protection of the information is not solely concerned with the protection of information systems. This master thesis therefore also reviews the possible threats to information that is used, transported and/or stored physically.

The extensive case study of the chemical company (Appendix A) focuses solely on threats to the confidentiality of information

Due to the competitive market in which the chemical company operates, and the nature of the initial question on how to protect intellectual property and information, the extensive case study of the chemical company (Appendix A) focuses solely on the mitigation of insider threats that could result in disclosure of information.

1.5. Master thesis structure

The structure of this master thesis report, based on the foregoing sections, is schematically represented in Figure 1. The structure explains the arrangement of the sections in accordance with the treatment of the central research questions.

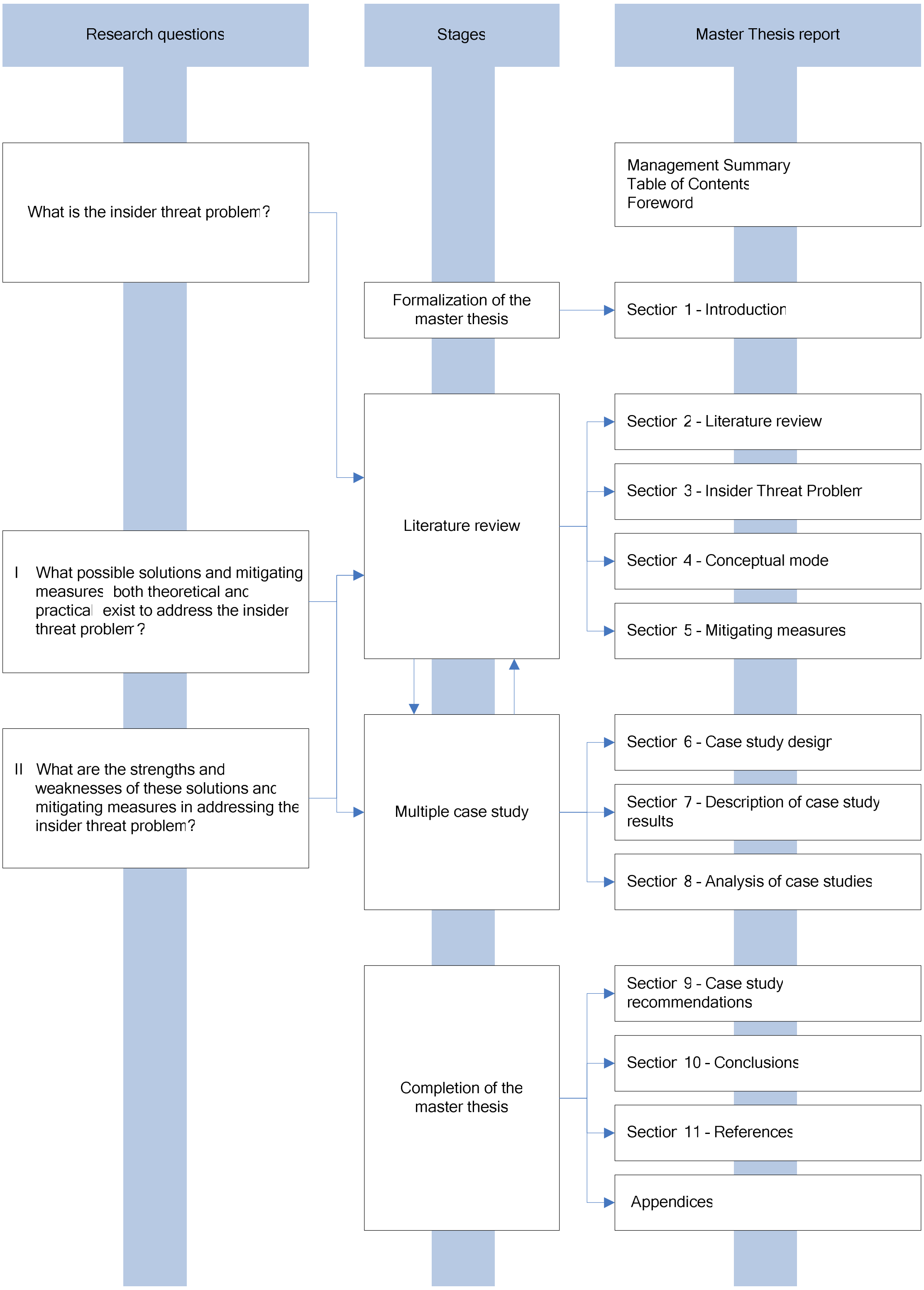

Research questions
Stages
Master Thesis report
What is the insider threat problem?
Management Summary
Table of Contents
Foreword
Formalization of the master thesis
Section 1 - Introduction
Literature review
Section 2 - Literature review
Section 3 - Insider Threat Problem
Section 4 - Conceptual model
Section 5 - Mitigating measures
I What possible solutions and mitigating measures (both theoretical and practical) exist to address the insider threat problem?
II What are the strengths and weaknesses of these solutions and mitigating measures in addressing the insider threat problem?
Multiple case study
Section 6 - Case study design
Section 7 - Description of case study results
Section 8 - Analysis of case studies
Completion of the master thesis
Section 9 - Case study recommendations
Section 10 - Conclusions
Section 11 - References
Appendices

Figure 1: Structure of the master thesis

2. Literature review

The literature review reflects on all three of the research questions. The objective is to review previous research related to the research questions in order to refine it into a conceptual model. The results of the literature review will be processed in sections 3 to 5. Section 2.1 extensively describes the search methodology that is used, and section 2.2 gives an overview and synthesis of the search results. The overall quality of this literature review is increased by looking at peer reviewed sources, which went through a blind review process.

2.1. Search methodology

To attain quality rather than quantity, the literature review follows a systematic methodology:

Search engine

The choice of the search engine determines which journals are covered. According to Schwartz & Russo (2004) Scopus.com and Web of Science both cover 92% of the top 25 IS Journals. In this literature review Scopus.com was used to search for scientific articles. By hand-searching the *Communications of the AIS* journal, 100% coverage should in fact be attained.

Search terms

Based on a brainstorm on the insider threat, some initial search terms were determined. In addition, some synonyms, different word forms or combinations were used. These were refined and/or extended, based on additional terms found in articles. Some of the terms that were initially used include, for example: ‘insider threat’, ‘insider misuse’, ‘insider attack’, ‘internal personnel threat’, ‘information theft’, ‘data leakage’ and ‘information protection’.

Selection criteria

- *Journal ranking*
  The IS journals, suggested by Schwartz & Russo (2004), were included in the literature review. Because of the limited number of IS Security research papers published in the leading IS journals, three additional IS Security specific journals were included. These three journals act as the three major publications in the field (Siponen & Willison, 2007): Computers & Security, Information Management & Computer Security and Information Systems Security.

- *Conference papers*
  Conference proceedings which covered the insider threat problem were also examined.

- *Citation analysis*
  The number of citations is an indicator of the relevance of a research paper, therefore papers that were often cited were selected. Next to top-down searching, driven by search engines and keywords, bottom-up searching was also applied. Bottom-up searching consists of forward- and backward citation analysis, which respectively describes papers that were referenced by or cited the papers that were found.

- *Publishing date*
  Due to the small amount of scientific literature found on the insider threat, no limitations on the publishing date were applied.

2.2. Search results

The application of selection criteria resulted in a large number of papers (Appendix B – 1). The papers that were found were evaluated and an initial selection was based on title and abstract. After this rough selection, the remaining papers were read. This resulted in exclusion of more papers. The resulting papers were compared and synthesized (Appendix B - 2). Forward and backward citation analysis resulted in additional (conference) papers that were not found using the initial keywords in Scopus.

The systematic literature review resulted in 29 useful scientific papers that describe (in part) the insider threat problem. The literature synthesis (Appendix B – 2) shows that most papers that were found included conceptual models and non-validated defense strategies. The topic of information security, and specifically research into the insider threat problem, has not been addressed by the leading IS journals (Siponen & Willison, 2007). The literature review confirms this and shows that most papers were in fact conference proceedings. Defining the problem boundaries is hard, not least because of the lack of appropriate definitions and contextual information, but also because of the lack of data for analysis, experimentation and, ultimately, validation of proposed solutions (Keromytis, 2008). According to literature this lack of data is driven by a variety of factors, the most prominent of which appears to be the sensitivity of the topic: organizations that have been the victims of insider attacks tend to handle such (known) incidents as quietly as possible (Hunker, 2008).

Although there was a lack of empirically validated models, it was possible to derive concepts that were commonly used. These concepts were used to synthesize the different papers. These concepts formed input for the sections that follow. Section 3 refers to the literature that relates to the characteristics of insiders and possible threats that can be posed by these insiders. Section 5 refers to the literature that describes measures for mitigating insider threats.

3. The Insider threat problem

"If one cannot define a problem precisely, how can one approach a solution, let alone know when the problem is solved?"
(Matt Bishop)

The results of the literature review, section 2.2, show that there are only a few publicly available empirical studies on insider attacks. The little existing peer-reviewed literature on the insider threat consists of non-validated insider threat models which address different aspects of the problem. Therefore, this section addresses the insider threat problem from both practical (e.g. best practices for information security) and theoretical perspectives.

3.1. Definitions

The terms information, information security, insider and insider threat have been mentioned a couple of times. This section describes and defines the terms more precisely.

3.1.1. Information security

Modern organizations make use of information systems to store, process and distribute valuable information assets. Information can be defined as data that have been converted into a meaningful and useful context for the receiver (Daft, 2000). What exact information is considered valuable depends on the organization, but examples are strategic information and intellectual property that give the organization a competitive advantage over its competitors.

It is therefore that information systems containing this information are confronted with a variety of threats originating from both the outside and inside. So called threat agents give rise to threats that exploit vulnerabilities in information systems and/or information security measures. These measures are imposed by organizations to reduce the risk to security of the information that is considered most valuable to them. Information security is a broad term for protecting valuable information against these possible threats. Figure 2 summarizes the general context of information security, in terms of concepts and relationships.

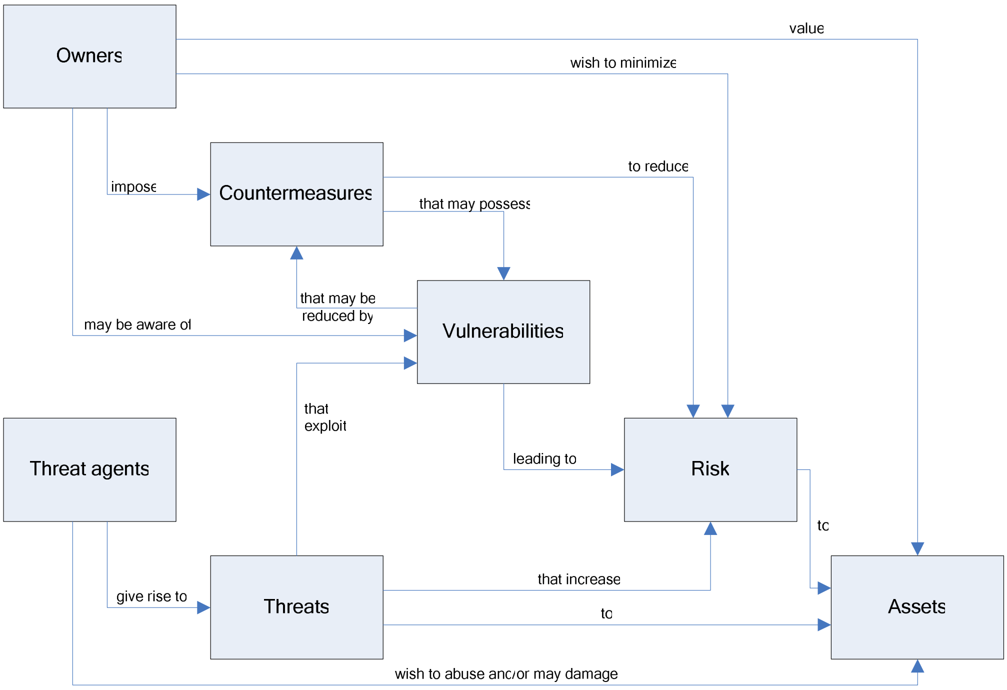


Figure 2: General security context, concepts and relationships (ISO/IEC 15408, 1999)

Failure of security could, for example, lead to unauthorized disclosure, modification, or interruption of information. These three examples relate to three properties of information security, commonly called confidentiality, integrity, and availability, respectively (ISO/IEC 15408, 1999). Ezingeard et al. (2005) describe these properties more precisely:

- *Confidentiality* means that information is accessible on a need-to-know basis and that unauthorized access is prevented.
- *Integrity* means that information is not modified or corrupted unauthorized, either accidentally or deliberately.
- *Availability* ensures that information is ready for legitimate use when it is required and that it will support the organization's ability to operate and accomplish its objectives.

Addressing the three security properties can be difficult due to conflicting interests of the parties that are involved. Medical institutions, for example, process large amounts of patient data. Although it is important to assure the confidentiality of these data, its availability is even more important. Information that is not readily available could directly result in loss of patients' lives (Sinclair and Smith, 2008). The focus on implementing measures to address threats to the confidentiality, integrity or availability of information could thus vary per organization. It is determined by their primary mission, goals and process. Figure 3 shows a schematic representation of the security focus, or information security profile, of an example medical institution. It is clear that the medical institution focuses more on availability and confidentiality, rather than integrity. Section 8.1.1 describes the information security profiles of the three case studies.

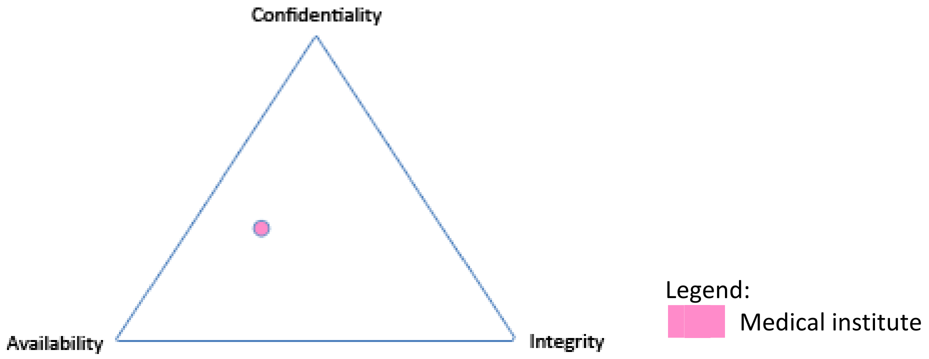


Figure 3: Example information security profile

It can be concluded that organizations that value their information need to safeguard it from threat agents that may also place value on their information in a manner that is contrary to the interest of the organization (ISO/IEC 15408, 1999). Recent security reviews (Richardson, 2008; Vadera et al., 2008) noted an average 40 to 50% of respondents having experienced corporate security incidents. Organizations therefore need to determine possible threats, or risks, to select appropriate counter- or mitigating measures. Appropriate in the sense that organizations can decide to accept the risk, or to further minimize it.

3.1.2. Insider

Who can actually be considered an insider, differs per organization (Predd et al., 2008). Not only system-specific characteristics, but also the organization's policies and values determine this. From the little existing peer-reviewed literature on the insider threat some definitions of an insider can be acquired. Table 1 contains a summary of these definitions.

Reference	Insider definition
Bishop (2005)	"Anyone with access, privilege, or knowledge of information systems and services". But also: "[…] anyone operating inside the security perimeter."
Butts et al. (2005)	"[…] an insider is any individual who has been granted any level of trust in an information system. […] What is important is that once users have been granted any authorized explicit right to the information system, they are now considered an insider".
Carroll (2006)	"[…] what is meant is any and all persons that have access to an organizations information including people such as contractors, temporary employees and the like".
Predd et al. (2008)	"Insider: someone with legitimate access to an organization's computers and networks. For instance, an insider might be a contractor, auditor, ex-employee, temporary business partner, or more".
Schultz (2002)	"[…] insiders would usually be employees, contractors and consultants, temporary helpers, and even personnel from third-party business partners and their contractors, consultants, and so forth".

Table 1: Literary references to the definition of an insider

The definitions summarized in Table 1 show some key characteristics that distinguish insiders from outsiders. These key characteristics are described below.

- ***Trust***
  Insiders are trusted persons. These trusted persons are usually employees, but could also be contractors and consultants, temporary helpers and even personnel from third party business partners that have formal or informal business relationship with the organization (Schultz, 2002; Predd et al., 2008; Pfleeger, 2008). The difference with an outsider is the fact that insiders can be trusted because they are assumed to be part of the organization's culture, may have signed a secrecy agreement and/or are assumed to pursue goals that are in the interest of the organization.

- ***Access***
  Insiders have legitimate access. It is important to distinguish legitimate from authorized access (Brackney and Anderson, 2004): a service technician or janitor may have legitimate access to offices, but may actually not be authorized to glance through documents that are left on desks. Legitimate access can result in physical access (i.e. janitor or visitor), network access (e.g. remote access) or both (e.g. employee working in an information system at the office).

- ***Knowledge and skills***
  Insiders have knowledge of information, information systems and services used in organizations (Wood, 2000; Bishop, 2005). This knowledge is not only limited to information systems but also includes knowledge from valuable information that is stored within them and the procedures and security measures that have been taken to protect the information. Because they have knowledge about the security measures and policies, insiders have the ability to violate them. This enhances the chances to go undetected.

  Magklaras and Furnell (2002) classify insiders in system roles. The basic criterion for classifying persons in the system role dimension is the type and level of system knowledge they possess; varying from *system masters* that have full administrative privileges to *advanced users* that do not have these privileges but possess substantial knowledge and privileges of system internals and *application users* that are likely to be able to abuse information that is related to the application they run.

Insiders are also considered to have the necessary skills to perform their jobs (Wood, 2000). Insiders have therefore not only knowledge of information, information systems and services used in the organization, but also an enhanced ability to misuse them compared to outsiders.

- ***Security perimeter***
  Insiders operate within the security perimeter of the organization (Bishop, 2005). The perimeter can be viewed from both a physical and logical perspective. For example, there may be logical insiders who are physically outside, and physical insiders who are logically outside (Neumann, 1999). It is however difficult to maintain a hard distinction between outsiders and insiders on this basis, due to all the outsourcing occurring (Schultz, 2002) and the increased level of connectivity offered by the convergence of mobile computing (Magklaras and Furnell, 2002).

It can be concluded that the main distinction between insiders and outsiders is the fact that insiders are trusted (Butts et al., 2005). These trusted insiders include employees but also, due to collaboration across companies (i.e. outsourcing activities), contractors and consultants, temporary helpers and third party business partners (Schultz, 2002). Trusted insiders have legitimate access to an organization's information (Brackney and Anderson, 2004; Carroll, 2006; Predd et al., 2008). In addition, insiders have knowledge about security measures and policies, which improves their ability to violate them.

For the purpose of this master thesis report, the insider will be defined as: *a trusted employee, temporary helper, contractor or consultant who has legitimate access to information and has knowledge about security measures that protect that information.*

3.1.3. Insider threat

Threats to valuable information are posed by so called threat agents that could originate from both the outside and inside (Figure 2, section 3.1.1). Research shows that although attacks originating from the outside, such as hacking attempts or viruses, have gained a lot of publicity, insider threats pose a significantly greater level of risk (Schultz, 2002; Baker et al., 2008).

The existing literature on the insider threat problem uses either the term 'insider attack' or 'insider threat'. Table 2 summarizes the literary references to definitions used for describing both insider attacks and insider threats.

Reference	Term	Definitions
Anderson et al. (2000)	Insider attack	"Any authorized user who performs unauthorized actions that result in loss of control of computational assets".
Bishop (2005)	Insider attack	"malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems"
Carroll (2006)	Insider threat	"Insider threats can be either intentional or unintentional".
NIST SP800-30 (2001)	Insider threat	"the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability"
Predd et al. (2008)	Insider attack	"[…] an insider's action that puts an organization or its resources at risk".
Schultz (2002)	Insider attack	"An insider attack is considered to be deliberate misuse by those who are authorized to use computers and networks". […] "inside attackers are those who are able to use a given computer system with a level of authority granted to them and who in so doing violate their organization's security

Reference	Term	Definitions
		policy”. “An insider attack can be defined as the intentional misuse of computer systems by users who are authorized to access those systems and networks”.

Table 2: Literary references to the definition of insider attacks and insider threats

There is a difference between the two terms used. The insider attack is the actual misuse itself performed by an insider and can be either successful or not. The attack is in fact the sequence of events or actions that result in use (e.g. compromise) of information that is not in accordance with the organization’s security policy. The insider threat is the potential for an insider to perform an attack. Insiders can either intentionally or unintentionally exploit vulnerabilities (NIST SP800-30, 2001; Bishop, 2005; Carroll, 2006) Vulnerabilities can be defined as flaws or weaknesses in system security procedures, design, implementation or internal controls that could be exercised and result in a security breach or a violation of the system’s security policy (NIST SP800-30, 2001; Schultz, 2002).

Based on the definition of an insider, and for the purpose of this master thesis, the insider threat can be defined as: *the potential for trusted employees, temporary helpers, contractors or consultants who have legitimate access, to exploit vulnerabilities and who in doing so violate the organization’s security policy*.

3.2. Insider classifications

This section describes the core of the insider threat problem. It starts with a classification of insider motivation and goals, which shows that insider threats can be posed either intentionally or unintentionally and could end up in disclosure, modification or interruption of information. Subsequently the focus is on the type of actions that insiders can carry out to pose threats.

3.2.1. Classification of insider motivation and goals

Not all insiders give rise to insider threats. It is good to know that most of the employees, contractors and consultants can actually be trusted and thus do share the same interest in safeguarding valuable information of the organization. It cannot be ruled out however that misuse of information systems, and information stored within them, occurs. Although most of the existing literature on the insider threat problem uses the term malicious when referring to these exceptions (Wood, 2000), it should be noted that not all cases of misuse are based on malicious intents.

Insider threats can also be posed by accident (Albert and Dorofee, 2001; Magklaras and Furnell, 2002; Carroll, 2006). These actions do, like those posed deliberately, violate the organization’s security policy (Schultz, 2002). The definition of an insider threat, stated in section 3.1.3, therefore refers to ‘violating the organization’s security policy’. Table 3 summarizes three insider motivation classifications, found in literature.

Albert and Dorofee (2001)	Capelli et. al (2006)	Wood (2000)
Vandals People who attack computer systems to cause damage. **Terrorists** People who attack computer systems to cause fear for political gain.	**Insider IT Sabotage** In these cases the insiders misused authorized access to systems or networks with the intention of harming an organization.	**Provoke change** In this case the malicious insider is invoking some sort of change in the organization (i.e. a change in the policy).

Albert and Dorofee (2001)	Capelli et. al (2006)	Wood (2000)
Disgruntled employees People within the organization who deliberately abuse or misuse computer systems and their information. **Attackers** People who attack computer systems for challenge, status or thrill.		**Personal motive** In this case the malicious insider might try to exact some sort of revenge against the organization. **Subversion** The malicious insider might try to subvert the mission of the target organization.
Criminals People who attack computer systems for personal financial gain.	**Fraud** In these cases the insiders intentionally misused authorized access to systems or networks with the intention of obtaining property or services from an organization unjustly through deception or trickery.	**n/a**
Competitors People who attack computer systems for economic gain. **Spies** People who attack computer systems for political gain.	**Theft of Information (Espionage)** In these cases the insiders intentionally misused authorized access to systems or networks with the intention of stealing confidential or proprietary information from an organization.	**Profit** In this case the malicious insider is motivated by some party that is paying the insider to disrupt or leak the information.
Non-malicious employees People within the organization who accidentally abuse or misuse computer systems and their information.	**n/a**	**n/a**

Table 3: Literary references to insider motivation classifications

The insider motivation classifications by Albert and Dorofee (2001), Capelli et. al (2006) and Wood (2000) show that the goals of the insiders can vary from disclosure (e.g. profit or theft), modification (e.g. fraud) and interruption or destruction of information (e.g. sabotage). These results are directly related to the information security properties: confidentiality, integrity and availability, respectively. In addition, the classifications show that threats can be either based on personal motives (i.e. economic gain, revenge) or motivated by some third party (i.e. information leakage).

3.2.2. Classification of malicious insider actions

Malicious insiders deliberately misuse information. Because of their malicious intents they are willing to take risks (risk from the perspective of the insider), follow a certain process and use different actions to accomplish their goals (Wood, 2000). Their ultimate defeat is to be discovered before they have mounted a successful attack. Wood therefore concludes that malicious insiders generally work alone, and will only employ others to the extent necessary. To mount a successful attack, the malicious insider follows a basic, predictable process:

- Someone becomes motivated to attack.
- The malicious insider identifies the target.
- The malicious insider plans the operation.
- The malicious insider launches the attack.

Malicious insider attacks can be predicted not only by recognizing the above process, but also by some potential indicators that were mentioned by Schultz (2002):

- *Deliberate markers.* Attackers sometimes leave deliberate markers to make a "statement". These markers can vary in magnitude and obviousness.
- *Meaningful errors.* Perpetrators, like anyone else, make mistakes in the process of preparing for and carrying out attacks. These mistakes could have been logged, although perpetrators can also try to erase all the evidence in the relevant log files (Schultz, 2002; Capelli et al., 2006).
- *Preparatory behavior.* In this case Schultz refers to the preparatory phase of an attack mentioned by Wood (2000).
- *Correlated usage patterns.* Correlated usage patterns are patterns of computer usage that are consistent from one system to another. A perpetrator may, for example, use a command to search on dozens of systems for files with particular words in them.
- *Verbal behavior.* Verbal behavior, either spoken or written, can provide an indication that an attack is imminent. Examples of such verbal behavior are email messages in which someone describes hostility towards an employer or statements to colleagues (Capelli et al., 2006).
- *Personality traits.* This indicator links to research on the psychological make-up of convicted perpetrators. It is suggested that personality factors (particularly introversion, stress handling and frustration) can be used in predicting insider attacks. A survey by Capelli et al. (2006) reveals that over half of the cases of sabotage were caused by insiders who acted out of revenge for some negative event. Examples of negative events include job termination, new supervisors, transfers or demotions, and dissatisfaction with salary increases or bonuses.

An insider threat can be posed in different manners: insiders can choose to carry out different types of actions to exploit vulnerabilities in information systems and/or information security measures. Anderson (1980) describes three types of malicious insiders, in addition Butts et al. (2005) describe four types of actions that malicious insiders may perform (Table 4):

Malicious insider types (Anderson, 1980)	Malicious insider actions (Butts et al., 2005)
Masquerader An insider with full access to a computer system who impersonates a legitimate user (e.g. through another legitimate user's identification and password that he may have obtained).	**Alteration** Alteration occurs when a malicious insider changes another user or object's rights in an unauthorized way. **Elevation** Elevation takes place when a user obtains unauthorized rights in the system. An example of this is someone trying to acquire administrative privileges. There are different ways malicious insiders may try to accomplish this: automated attacks, social engineering.

Malicious insider types (Anderson, 1980)	Malicious insider actions (Butts et al., 2005)
Misfeasor Misfeasance involves the misuse of authorized access both to the system and to its data. **Clandestine** This insider has or can seize supervisory control and as such can either operate below the level at which logs are taken or can use privileges to erase the logs.	**Distribution** Distribution captures the transfer of protected information to an unauthorized entity. This occurs when a user has appropriate system rights and a need to know, such as access to a file. When a right or entity is transferred to someone or something that is not supposed to have them, it is called distribution. **Snooping** Snooping addresses obtaining unauthorized information on a user or object. This action is similar to Distribution except the user has appropriate system rights without a need to know. This takes place when a user has permissions by the system access controls but the event should not take place because it violates organization policy.

Table 4: Malicious insider types and actions

The three types of malicious insider types (Anderson, 1980) and the malicious insider actions described by Butts et al. (2005) show that malicious insiders can perform both authorized and unauthorized actions. A misfeasor, for example, performs authorized actions as far as the system is concerned. Unauthorized access can thus be the result of both authorized and unauthorized actions.

- **Misuse of authorized actions**
  A malicious insider can misuse authorized actions (i.e. physical access to buildings or authorized access to information systems).

- **Use unauthorized actions**
  Use of unauthorized actions can be, for example, obtaining authorized access from an authorized insider by stealing user credentials.

3.3. Insider threat profiles

The possible insider threats to information and/or information systems are represented in Figure 4. The different threat profiles are based on general insider characteristics, motivations and actions, discussed in section 3.1.2, 3.2.1 and 3.2.2 respectively.

According to the definition of an insider, stated in section 3.1.2, every insider has legitimate access. Figure 4 shows that this legitimate access may imply only physical access (i.e. janitor, visitor), network access (i.e. remote access from contractor) or both (i.e. employee working at the office in an information system). These different forms of access may result in threats that can be posed either intentionally or unintentionally. Making this distinction is important, because not all insider threats are posed with the intent of causing harm to the organization. Both intentional and unintentional threats can be carried out by misusing authorized actions to information or by the use of unauthorized actions. The result of the threats can either be disclosure (threat to confidentiality of information), modification (threat to integrity of information) or interruption and destruction (threats to the availability of information) of information.

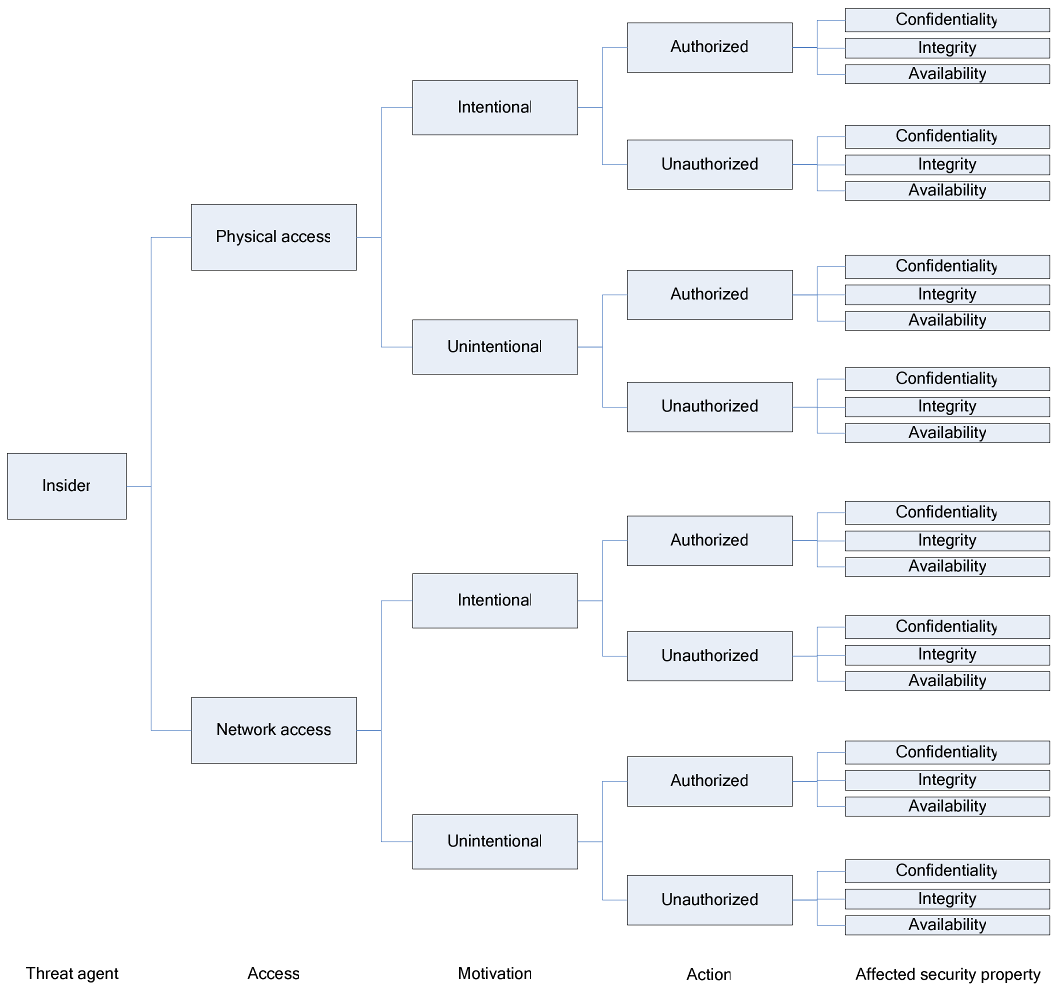


Figure 4: Insider Threat profiles (based on Albert and Dorofee, 2001)

In the subsections that follow, the threat profiles are explained more thoroughly by the use of example cases.

3.3.1. Intentional misuse of physical access

This category considers an insider who intentionally misuses physical access to information and/or information systems. The underlying motivation can be either sabotage, fraud or theft of information (Capelli et al, 2006). Table 5 shows what threats can be posed.

Threat		Example cases
TH01	Abuse physical access to transport and/or distribute information	▪ Taking valuable information (hardcopy, removable media) out of the organization
TH02	Abuse physical access to view information to which the insider is not authorized to	▪ A janitor or service technician viewing business confidential documents that are left on tables
TH03	Abuse physical access to sabotage information and/or information systems	▪ Compromise backup tapes and destroy source data ▪ Intentionally damaging equipment that is located on the workplace

Table 5: Possible treats posed by intentional misuse of physical access

3.3.2. Unintentional misuse of physical access

This category considers an insider who unintentionally misuses physical access to information and/or information systems. Table 6 shows what threats can be posed.

Threat		Example cases
TH04	Disclosure of valuable information due to loss	▪ Loss of information (hardcopy, removable media, laptop) that was taken outside by an authorized insider (e.g. theft by an outsider) ▪ Disclosure of thrown away information
TH05	Unintentional destruction of valuable information	▪ Throwing away valuable information

Table 6: Possible treats posed by unintentional misuse of physical access

3.3.3. Intentional misuse of network access

This category considers an insider who intentionally misuses network access to information and/or information systems. The underlying motivation can be either sabotage, fraud or theft of information (Capelli et al, 2006). Table 7 shows what threats can be posed.

Threat		Example cases
TH06	Abuse network access to transport and/or distribute information	▪ Sending business confidential information by email to an interested third party. ▪ Taking large amounts of business confidential information out of the perimeter, using an USB device. ▪ Using the remote connection (used for teleworking) to print large amounts of business confidential information at home, hotel or public place. ▪ Violaton of separation of duties principle
TH07	Abuse network access to alter information	▪ Abuse the rights to change bank account numbers in the central ERP system for financial interests ▪ Alter loggings to cover up tracks of recorded unauthorized actions. ▪ Create backdoor accounts for future use ▪ Elevate access rights of an friendly employee
TH08	Abuse network access to sabotage information and/or information systems	▪ Compromise backup tapes and destroy source data
TH09	Abuse network access to install malicious software	▪ Install a virus on a server in the network using local admin rights ▪ Place a logic bomb or malicious code in a piece of software code
TH10	Abuse authorized network access of an authorized insider (which enables the insider to exploit TH06 – TH09)	▪ Stealing user credentials from an authorized insider by using password sniffers. ▪ Take advantage of a computer that is left unlocked to impersonate another user
TH11	Abuse non-revoked network access (which enables the insider to exploit TH06 – TH09)	▪ Intentionally exploiting account management deficiencies (due to job changes) ▪ Intentionally exploiting a user account that was not revoked after job termination

Table 7: Possible treats posed by intentional misuse of network access

3.3.4. Unintentional misuse of network access

This category considers an insider who unintentionally uses network access to information and/or information systems. Table 8 shows what threats can be posed.

Threat		Example cases
TH12	Unintentional distribution and/or transportation using network access	▪ Disclosure of information by accidentally using reply-to-all on a mailing list ▪ Unintentional publishing of business confidential information on a new project by a trusted machine builder
TH13	Unintentional use of information system resulting in errors	▪ Inaccurate data entry, resulting in errors in financial systems
TH14	Use of authorized network access to accidentally install malicious software	▪ Install a virus on a server in the network using local admin rights
TH15	Unintentional use of unauthorized network access	▪ Sharing passwords with fellow insiders as a solution for business continuity during vacations ▪ Creating workarounds for non supported system actions ▪ Accidentally acquiring information that was left unattended by an insider (i.e. USB stick, documents or on screen)

Table 8: Possible treats posed by unintentional misuse of network access

3.4. Risk of insider threats

This subsection evaluates how serious the problem of insider threats is, based on the magnitude and frequency of occurrences as reported in literature. *Risk* (from the perspective of the organization) is a function of the *likelihood* that a given *insider* exploits a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization (NIST SP800-30, 2001). Section 3.4.1 describes scale and occurrence of an insider threat which is in fact the likelihood and section 3.4.2 discusses the impact of insider threats. Section 3.4.3 describes the actual risk computation and section 3.4.4 concludes with some remarks on risk minimization strategies that firms can apply to mitigate insider threats.

3.4.1. Insider threats: scale and occurrence

Schultz (2002) states that the 'myth' that "more attacks come from the inside than from anywhere else" traces back to old FBI statistics based on clunky mainframes and mini computers who had only a fraction of the network capabilities that today's machines have. In addition, Schultz notices that not many people were capable of attacking these systems, except for insiders. On grounds of these remarks, it was not strange that 80% of computer crime was believed to be the result of insider activity (Furnell and Phyo, 2003). Nowadays, the same FBI statistics reveal that insider activity is responsible for 40 to 50% of security incidents (Richardson, 2008). Other sources report lower figures (Table 9) but did not, for example, consider business partners as being insiders.

Survey	Reference	Description	Insider security breaches (%)
2008 CSI/FBI Computer Crime and Security Survey	Richardson, 2008	Survey: 433 respondents	44%
2008 Verizon Data Breach Investigations Report	Baker et al., 2008 (fig 2)	500+ cases of data breach and compromise	18%*
Information Security Breaches Survey 2008	Vadera et al., 2008	Survey UK Business: 1007 respondents	16%**

Table 9: Research on insider security breaches

* In addition, 39% of security breaches were caused by partners.

**According to 62% of the respondents, the worst security incidents were caused by insiders.

There is another problem with the figures shown in Table 9, because presenting the insider threat problem in this manner tends to create something of a false impression (Furnell and Phyo, 2003). First, the percentages presented above can be explained in several ways: the proportion of attacks originating from the outside is increasing; insider incidents are not being reported due to perceived risk of bad publicity; and more insiders remain undetected (Caruso, 2003; Hunker, 2008). Second, the percentage of incidents caused by insiders is only one part of the risk computation: the impact of those incidents is also important in explaining the risk of insider threats.

3.4.2. Impact of insider threats

The other part of the risk computation is thus the actual impact of insider threats. Indicators of the impact can be represented in terms of, for example, effects on annual losses (Furnell and Phyo, 2003) or the number of records compromised (Baker et al., 2008). However, next to the direct consequences of an insider threat, the organization can also suffer from indirect effects (Sinclair and Smith, 2008):

- *reputation risk that can dramatically impact stock prices and market shares*
- *business continuity* when attacks are destructive to systems or their availability
- *competitive advantage* which may be lost due to loss of intellectual property
- *loss of trust* from customers and business partners

Figure 5 shows that according to Baker et al. (2008), the percentage of security breaches caused by insiders was lower than those originating from outsiders but the impact exceeded that of an outsider by more than 10 to one. Schultz (2002) therefore rightfully concludes that more risky attacks come from inside.

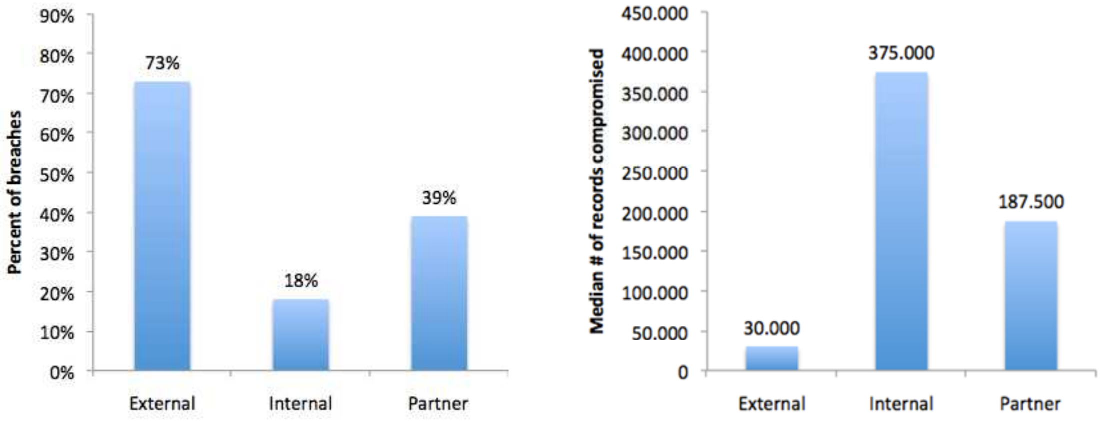


Figure 5: Sources of data breaches and the number of records compromised (Baker et al., 2008).

3.4.3. Risk computation: the insider threat problem

Based on the figures on the occurrence of the insider threat, and the impact of this threat, the actual risk of insider threats can be (roughly) computed. Table 10 shows an example computation based on the multiple case study by Baker et al. (2008).

Source	Likelihood	Impact (# of records)	Risk (pseudo)
External	73%	30.000	21.900
Internal	18%	375.000	67.500
Partner	39%	187.500	73.125

Table 10: The risk of data breaches by different sources (Baker et al., 2008)

The risk of data compromise by internal sources is 3 times higher than the risk of outside sources. The risk of partners, third parties that share a business relationship with the organization, even exceeds that of insiders. As acknowledged by Furnell and Phyo (2003) and Schultz (2002), the level of risk of the insider threat is still much higher than that exhibited by outsider threats.

3.4.4. Risk minimization strategies

After risks have been identified and assessed, organizations can choose between different risk minimization strategies. Bojanc and Jerman-Blazic (2008) identify four strategies:

- *Avoiding* results in eliminating the vulnerabilities or the assets exposure to the threat. This strategy is applied in cases when the severity of the impact of the risk outweighs the benefit that is gained from having or using the information.
- *Reducing* the assets exposure to the risk by implementing appropriate technologies and tools (such as firewall, antivirus systems, etc.) or adopting appropriate security policies (i.e. passwords, access control, port blocking). Reduction or ‘mitigation’ is the primary risk management strategy.
- *Transferring* the risk responsibility by partially shifting the risk to either outsourcing security service provision bodies or buying insurance.
- *Accepting* the security measures as a cost of doing business. Risk retention is a reasonable strategy for risks where the cost of investment or insuring against the risk would be greater over time than the total losses sustained.

Bojanc and Jerman-Blazic (2008) acknowledge that choosing between different strategies may involve trade-offs or using a combination of two strategies. In some cases, ideal use of the strategies may not even be possible. For the purpose of this master thesis it is assumed that organizations follow the strategy of mitigating (e.g. reduce) insider threats.

3.5. Summary

Organizations that value their information need to safeguard it from threat agents originating from both the outside and inside. Information security is the process of safeguarding the confidentiality, integrity and availability of information (Figure 6). Section 3.4.1 shows that although attacks originating from the outside, such as hacking attempts or viruses, have gained a lot of publicity, insider threats pose a significantly higher level of risk. Schultz (2002) rightfully concludes that the more risky attacks come from inside.

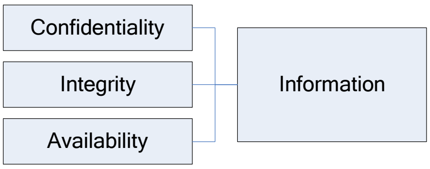


Figure 6: Information security properties

Insiders can pose more risky attacks because they are trusted and have the necessary access to be able to exploit vulnerabilities more easily. Employees, temporary helpers, contractors and consultants are all considered insiders. Insiders do not only have access, they also have knowledge about business processes, security measures and their vulnerabilities. This knowledge enables insiders to carry out actions such as the misuse of authorized access, but also to create ways to expand authorizations and/or misuse otherwise obtained authorized access. This gives insiders a higher probability to remain undetected and of being successful. Not all cases of insider misuse are based on malicious motivations. Insider threats can also be posed by accident. Whether an insider threat is deliberate or accidental depends on the motive of the insider. Malicious insiders can have either personal motivations or motivations that are initiated by outsider interests.

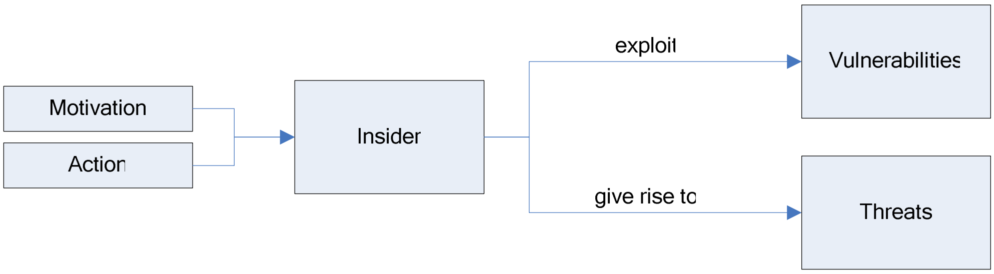


Figure 7: Insider threat characteristics

Survey results show that the insider threat problem is really a serious problem. Insider activities are responsible for 40 to 50% of security incidents (section 3.4.1). These percentages could, however, give a false impression. Insiders are more likely to remain undetected, and due to the perceived risk of bad publications insider attacks are not reported. Surveys (section 3.4.2) also reveal that the impact of security incidents posed by insiders exceeds that of outsiders either directly or indirectly. Direct effects of successful attacks are for example effects on annual losses or compromised records, indirect effects could for example be the loss of reputation, loss of competitive advantage or effects on business continuity.

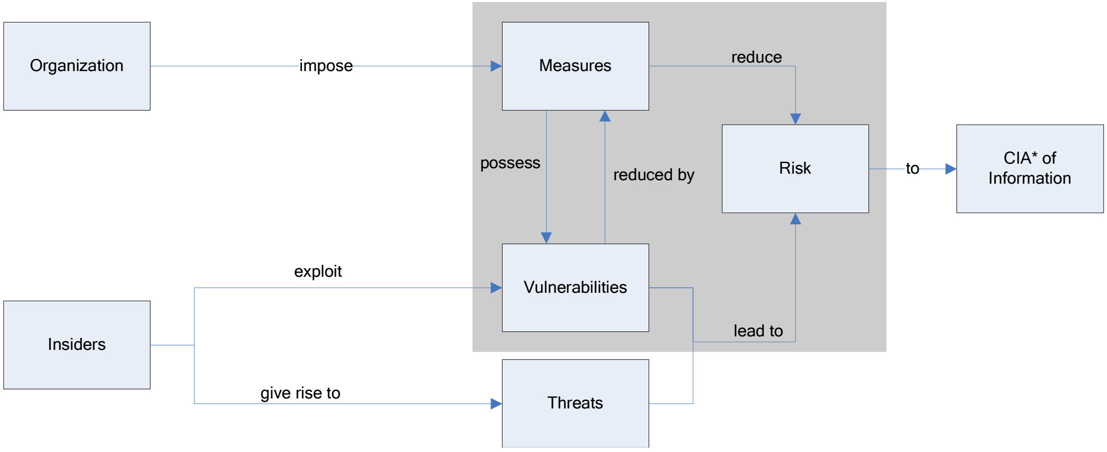
To mitigate the risks caused by insiders, organizations can choose to apply different risk minimization strategies. Organizations can for example transfer the risk by outsourcing the information security process. For the remain of this master thesis it is assumed that reduction or mitigation is the primary risk management strategy.

It should be noted, however, that the scientific literature that was referred to in this section, is not yet mature. The literature review in section 2 showed that there is a lack of data on insider attacks that could help validate the definitions, classifications and conceptual models that were found in literature. In section 4, therefore, a conceptual model is presented that is derived from both theory and best practices.

4. Conceptual model

In section 3 the various concepts of the insider threat problem, derived from the literature review in section 2, were extensively described. Due to the limited availability of empirical evidence, the insider threat problem was addressed from both a theoretical and practical perspective.

The theoretical perspective extensively describes the information security properties, general insider characteristics and possible insider threats. The practical perspective is based on a best practice for information technology security evaluation; the ISO/IEC 15408. This standard describes a general security context which states that organizations impose measures to safeguard their information from threats that originate from both the outside and inside. Insiders give rise to threats, and thereby exploit vulnerabilities in security measures, that lead to risks for the confidentiality, integrity and availability of information. Figure 8 combines the theoretical and practical perspectives into a conceptual model that represents the insider threat problem. It includes the concepts that were discussed in the previous section.



*CIA: Confidentiality, Integrity and Availability of information
Figure 8: Conceptual model of the insider threat problem

The grey marking in the conceptual model represents the topics that are addressed in the sections that follow. Section 5 extensively describes the measures that organizations can apply to address insider threats according to theory, including the vulnerabilities of these measures. The multiple case studies, covered in section 6, 7 and 8, continues with an evaluation of the application of measures in practice. The conceptual model will guide the initial collection of data by case study interviews.

5. Mitigating measures to address insider threats

”The only truly secure system is one that is powered off,
cast in a block of concrete and sealed in a lead-lined room with armed guards”
(Gene Spafford)

This section describes the measures that firms can take to mitigate the insider threat problem. Section 5.1 describes the classification of measures and in section 5.2 these measures are described more extensively. Section 5.3 relates the measures to the specific threats that are posed by insiders.

5.1. Classification of mitigating measures

Insider threats are posed by insiders that exploit vulnerabilities in information systems and/or information security measures. On the one hand information security measures reduce the vulnerabilities that lead to a risk of misuse of information; on the other hand these same measures may in fact possess vulnerabilities that lead to other risks (ISO/IEC 15408, 1999).

5.1.1. Technical-, Formal- and Informal controls

In the available literature many authors emphasize that information security is not only a matter of technical controls or measures (Melara et al., 2003). Information security involves people, organizational factors, technology and the working environment. To cover all these aspects, Dhillon (1999) has proposed three kinds of security controls to effectively secure an information system:

- *Technical controls* include mechanisms to protect information systems from attacks or incidents. Antivirus software, access controls, backups, recovery and audit software, for example (Melara et al., 2003).
- *Formal controls* include business structures and processes that ensure the correct general conduct of business and reduce the probability of an incident or an attack, or at least minimize its impact. For example, separating the security organization from other IT departments, designing correct separation of duties and therefore access rights and privileges, designing and controlling the appropriate employee-supervisor relationship, routine risk evaluations, etc (Melara et al., 2003).
- *Informal controls* essentially deal with the culture, value and belief system of the organization. An organizational culture in which it is possible to understand management’ s intentions, and which is conducive to developing a shared vision and other informal objectives, would make members of the organization more committed to their activities and to the success of the organization as a whole. Informal controls might be created, for example, by increasing awareness of security issues through education and training programs (Melara et al., 2003).

Individual controls in each of the three categories, though being important, must complement each other (Dhillon, 1999). Recent research confirms this and indicates that successful defense against insider threats depends on both technical and behavioral solutions (Martinez-Moyano et al., 2008).

5.1.2. Prevention, detection and response to insider threats

Besides the distinction between technical-, formal- and informal controls, other authors (Schultz, 2002; Carroll, 2006) classified measures based on their timing:

- *Prevention.* Measures which are aimed at avoiding occurrence of an insider threat, including measures to predict insider attacks on the basis of potential indicators. Carroll (2006) states that regulatory compliance is forcing organizations to reconsider how risk management is approached; internal policy is the base for regulatory compliance and insider incident prevention. Policy defines and governs actions and behaviors of personnel within an organization. However, policy by itself is not very useful if it not backed by consequences. These consequences have the greatest impact to the insider threat (Carroll, 2006).
- *Detection.* Measures which are aimed at discovering the presence of an insider threat when the actual attack occurs or has already occurred. Several methods are available to detect outsider attacks; the detection of insider actions is, however, much harder (Carroll, 2006). Insider actions can be detected by the use of monitoring and logging tools, whistle blower policies and honeypots.
- *Response.* Measures which are employed to deal with an insider threat once it has occurred. These measures can be corrective and repressive, to minimize the effect. Organizations can also apply responsive measures to insiders concerned. At first sight, response to an insider threat seems quite simple: a lawsuit. In reality, however, the response to insider threats can be rather complicated. Organizations tend to keep the threat out of the public eye for fear of bad press (Carroll, 2006). In cases where lawsuits were the response, the organizations did not recover any of the damages, but punished the insiders concerned. For the public this may look like the organization is doing all that it is capable of to protect itself (Carroll, 2006).

Although detection of insider threats is desirable, it is post hoc in nature (Schultz, 2002). Therefore, according to Schultz, the most pressing need is developing the ability to predict (thus prevent) insider attacks. In section 3.2.2 some potential indicators (i.e. deliberate markers, verbal behavior) were proposed which apply for insider threat prevention. Prevention can be achieved by, for example, educating the organization’s members, so that these indicators can be recognized and reported timely.

5.2. Categorization of measures

In section 5.1 two classifications of measures were proposed. These included the distinction between formal, informal and technical controls by Dhillon (1999) and the classification based on the timing of measures: prevention, detection and responsive (Schultz, 2002; Carroll, 2006). In Figure 9 these classifications of measures are combined with the properties of information security that are addressed: confidentiality, integrity and availability, described in section 3.1.1.

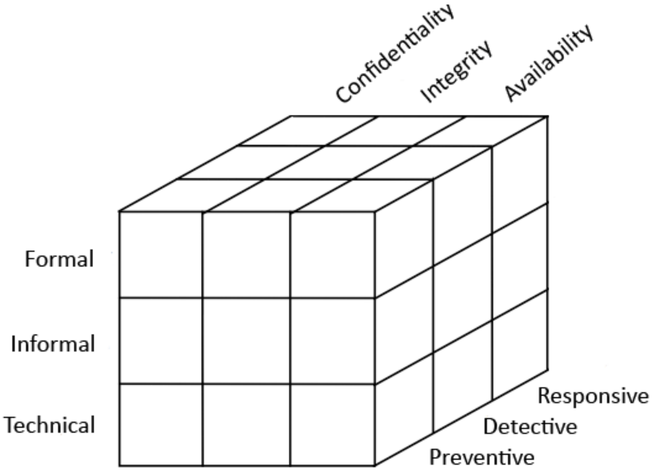


Figure 9: Schematic representation of categorization of measures (based on cubic of Bautz, Overbeek 2002)

Recent research suggests that successful defense against the insider threat depends on both technical and behavioral solutions (Martinez-Moyano et al., 2008). Dhillon (1999) already suggested that these solutions should complement each other. It seems valuable, therefore, to categorize measures based on the distinction between formal, informal and technical controls.

This categorization can be extended by evaluating the security properties that are affected by implementing the measures. Some measures address all security properties, some are more specific and address for example only confidentiality. Organizations may wish to focus specifically on one of the security properties because, for example, their risk assessment showed high risks to the availability of information. Therefore, the security properties should also be included in the categorization of measures. The measures to mitigate the insider threat problem can thus be categorized in accordance with the classification of Dhillon (1999) and the properties of information security. This categorization is applied in the table below (Table 11).

	Affected information security properties		
Measures	Confidentiality	Integrity	Availability
Formal measures	Security policy; Pre-employment screening; Third party contracts; Physical access control; Dual control; Separation of duties; Revocation of authorizations; Least privilege; Incident registration; Audit;		
	Legally binding documents; Clean desk policy; Restrictions on removable media;	Security in Software Development Life Cycle;	Contingency planning;
Informal measures	Security education; Manage organizational culture;		
Technical measures	Clear screen policy; Authentication; Role Based Access Control; Monitoring and Logging; Intrusion Detection System;		
	Encryption; Watermarking; Data Leakage Protection suite;	Application control; Antivirus;	Backup;

Table 11: Categorization of mitigating measures

The mitigating measures in Table 11 are categorized into formal, informal and technical controls. In addition, each of the measures is related to affected security properties. As was stated before, some measures affect all security properties and some address only one specific security property. The measures that are mentioned in Table 11 are extensively described in appendix C.

5.3. Measures versus threats matrix

This section describes the degree to which the measures that were found in literature mitigate the threats that insiders could pose. The determination of the degree of mitigation is based on the description of the measures in Appendix C. Appendix C describes the measures more extensively and includes also the effectiveness and trade-offs of these measures that are derived from the literature review.

The measures that were described in Table 11 are carried over to Table 12. This table shows whether the measures are preventive, detective or responsive and to what degree they mitigate the threats. The timing aspect determines the focus of the mitigation. Monitoring and logging cannot, for example, prevent an actual attack but it does actually help to identify the perpetrator. More weight has been given to measures that are preventive, compared to those that are detective and responsive. In addition, the degree of mitigation is also determined by the restrictiveness of the measure. The restrictiveness of the measure is the degree to which the insider is able to circumvent the measure.

		Timing			Threats														
					Physical access to distribute information	Physical access to view information	Physical access to sabotage information	Disclosure of information due to theft	Unintentional destruction of information	Abuse network access to distribute	Abuse network access to alter information	Abuse network access to sabotage info.	Abuse network access to install malicious	Abuse obtained network access	Abuse non-revoked network access	Unintentional distribution using network	Unintentional misuse of information system	Accidental install of malicious software	Unintentional use of unauthorized access
Measures		Preventive	Detective	Responsive	TH01	TH02	TH03	TH04	TH05	TH06	TH07	TH08	TH09	TH10	TH11	TH12	TH13	TH14	TH15
F01	Security policy	x		x	M	M	L	M	L	M	M	M	M	L		M		M	L
F02	Pre-employment screening	x			L	L	L			L	L	L	L	L					
F03	Third party contracts	x		x	M	L	L			M	L	L	L						
F04	Legally binding documents	x		x	M	L				M									
F05	Physical access control	x	x		M	M	**H**												
F06	Dual control	x					L			L	M	M					L		
F07	Separation of duties	x									M	M					L		
F08	Least privilege	x								L	L	L	L		L	L	L	L	L
F09	Revocation authorizations	x													**H**				
F10	Clean desk policy	x			**H**	**H**	L												
F11	Restrictions remov. media	x			**H**			**H**		**H**						M			
F12	Contingency planning			x			M		M		L	M	L				L	L	
F13	Audit		x	x						M	M	M	M	M	M	L	L	L	L
F14	Security in SDLC	x									M	M							
F15	Incident registration		x	x	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
I01	Security education	x	x		M	M	M	M						M		M		M	**H**
I02	Manage org. culture	x	x		L	L	L	L	L	L	L	L	L	L	L	L		L	L
T01	Clear screen policy	x												**H**					
T02	Authentication	x			M	M	M			M	M	M	M	**H**					
T03	Role Based Access Control	x								L	L	L	L						
T04	Antivirus	x											**H**					**H**	
T05	Encryption	x			M			**H**								**H**			
T06	Watermarking	x	x		M			M		M						M			
T07	Monitoring and logging		x	x						M	M	M	M	M	M	M	M	L	M
T08	Intrusion Detection System		x	x						L	L	L	L	L	L				
T09	Data Loss Prevention suites	x	x							**H**						**H**			
T10	Backup			x			**H**		M		M	**H**	M				M	M	
T11	Application controls	x									M						**H**		

Legend: L Low mitigation M Medium mitigation **H** High mitigation
F Formal measure I Informal measure T Technical measure

Table 12: Measures versus threats matrix

5.3.1. Analysis of the effectiveness of measures

Table 12 gives an overview of the effectiveness of measures in terms of the degree to which the threats are mitigated. Most of the formal measures have low- or medium mitigating effects, except for physical access control, the clean-desk policy and the restrictions on the use of removable media. These measures are more stringent and therefore result in restrictions on the freedom of insiders to undermine policies that are for example described in the security policy. The security policy is important to set guidelines and to describe appropriate behavior, including penalties to non-compliance, but it does not restrict the abilities of insiders to pose threats. Other measures such as the principle of least privilege cannot prevent insiders with appropriate authorizations to misuse these authorizations; the principle can only mitigate the impact of this misuse.

Informal measures are related to the communication of both the formal- and technical measures, and creating awareness upon the topic of security in general. Although security education is able to mitigate some of the threats, in most cases it is preventive in nature; it is not able to effectively mitigate threats by for example malicious insiders. Security education and managing the organizational culture can only create an environment in which trusted insiders are aware of the possible threats and are willing to report suspicious incidents. These measures are thus more focused on the detection of insider threats.

Like the clean-desk policy and the restrictions on the use of removable media, some technical measures also result in restrictions on the freedom of insiders to use information and/or information systems. The clear-screen policy and the use of stronger authentication methods on both the physical and logical perimeter restrict the ease of access to valuable information and are therefore more effective to mitigate threats. Encryption can effectively mitigate threats that are related to the disclosure or loss of valuable information and application controls effectively mitigate threats that are related to misusing information systems to alter information. Although backup measures are effective they are reactive and are thus capable of recovering from threats that were posed. Monitoring and logging is an important control to enable the organization to discover and investigate suspicious insiders, it is therefore an effective measure to prosecute malicious insiders.

5.3.2. Analysis of the likelihood of threats

The threats that could be posed by insiders that have physical access can be mitigated effectively by a combination of measures such as physical access control, clean desk policies and restrictions on the use of removable media. The threats that exploit authorized network access are however more challenging to mitigate. Restrictions on the use of removable media may restrict the possibilities of transporting valuable information outside the organization, but other vulnerabilities remain uncovered. Even with a combination of the principle of least privilege and separation of duties, authorized insiders are able to exploit their access rights. To mitigate these threats, a combination of monitoring and logging and role based access control can be applied, to identify misuse including the actual perpetrator.

Obtaining authorized network access from another insider, through the use of a computer that was left unattended or the use of stolen user credentials can be mitigated effectively by a combination of the application of stronger authentication and a clear screen policy.

The threats that are related to unintentional misuse of network access can partly be mitigated by stringent application controls, which check upon validity of input and output, and security education that communicates appropriate use of information in accordance with the security policy.

5.4. General remarks on mitigating measures

Overall, the measures versus threats matrix (section 5.3) shows that only a small number of threats can actually be mitigated effectively. The key characteristics of insiders, being trusted and therefore having legitimate access to information, make it hard to effectively mitigate threats posed by these insiders. It is particularly revealing that this opinion is shared by many experienced security practitioners in the financial services industry, a sector that has both had considerable experience with malicious insiders and is a very aggressive adopter of new security technologies and practices (McMormick, 2008).

The fact that insiders have legitimate access, gives them extensive possibilities to carry out activities to distribute and/or transport the information, alter the information or even destruct it. Although measures such as the least privilege principle, dual control and separation of duties exist, insiders are still capable of exploiting authorizations that they need for business purposes. There is no single solution to the insider threat; measures can only be implemented to reduce the risk.

Point of departure for the implementation of the measures found in literature is a proper risk assessment where risks are identified and assessed (Capelli et al., 2006). Based on the risks that are identified, the organization chooses appropriate risk minimization strategies (section 3.4.4). It is important to pay attention to the advantages and disadvantages of implementing measures:

- Having or using the valuable information should outweigh the cost of implementing the measures that need to protect it
- Measures imply significant changes and restrictions on the execution of business tasks, therefore it is important to maintain a workable situation
- Implementing measures gives the organization more control over its valuable information, however, more control may result in a feeling of distrust

The implementation of measures should be accompanied with communicating these measures through security education and managing the security culture. The security policy defines and governs the actions and behaviors of personnel within the organization and should therefore act as a guide that can be consulted during and after security education.

5.5. Summary

Organizations impose measures to reduce the risks to the confidentiality, integrity and availability of information. Recent research suggests that successful defence against insider threats depends on both technical and behavioural solutions (section 5.1.1). In section 5.1.1 it is also suggested that to effectively secure information systems, formal-, informal- and technical measures should be applied. Individual controls in each of the categories, though being important, must complement each other.

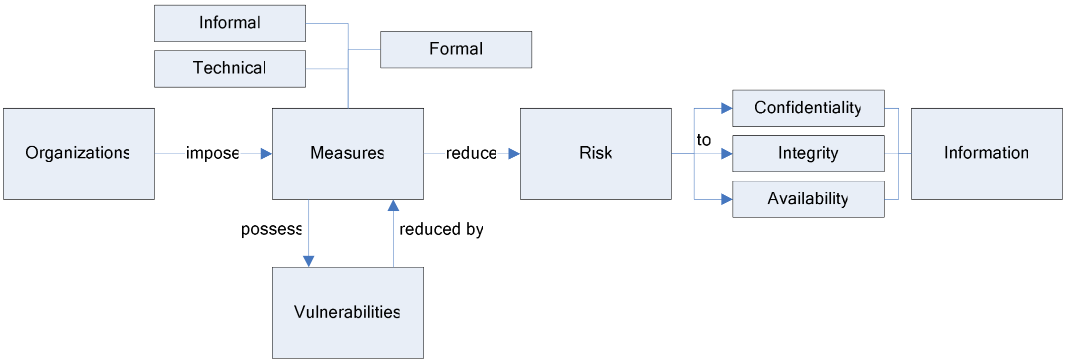


Figure 10: Mitigation measures to reduce risks caused by insiders

Organizations can thus impose some basic measures that could reduce the occurrence of insider threats to a minimum. It is advisable to implement a multi-layer defense of formal, informal and technical measures. A risk assessment and analysis should identify the possible threats to information security and an appropriate risk minimization strategy should be applied to address the identified risks. Pre-employment screening can help to prevent hiring malicious insiders. Security education, the most cost effective measure (Appendix C – 2), facilitates corporate security awareness that could help to recognize the indicators of insider threat occurrence. This security education, should be based on a security policy, that defines and governs appropriate behavior towards information and information systems. Strict access control and revocation of authorizations can help reduce the impact of insider threat occurrence. Monitoring and logging are important to detect misuse and to be able to prosecute the identified misuser.

Measures can only reduce the insider threat problem; there is no single solution to counter insider threats. On the one hand information security measures reduce the vulnerabilities that lead to risks, on the other hand these measures possess other vulnerabilities that could be exploited (section 5.1). In addition, there are of course costs and efforts related to the application of security measures. These costs and efforts include not only financial expenditures on IT resources, but also reductions of productivity and creativity, and an erosion of trust between employer and employees. Therefore, having or using the valuable information should outweigh the cost of implementing the measures that need to protect it.

6. Case study design

Based on the conceptual model, knowledge from practice will be acquired by conducting multiple case studies. The use of case studies is extensively described by Pare (2004). Pare defines case studies as an empirical inquiry that investigates a contemporary phenomenon within its real life context, especially when the boundaries and context are not clearly evident. In order to cope with problems of subjectivity and inability to generalize and replicate, a theory driven approach is chosen.

6.1. Sources of evidence

Multiple sources of evidence are available. To strengthen the case study research, complementary evidence is acquired. This will also increase credibility and reduce bias.

- *Interview*
  Interviews are the most important source of information in this multiple case study. It is important to include more than one perspective; therefore multiple interviews with different stakeholders are included. The interview questions are based on the conceptual model (section 4) and are addressed in section 6.3.
- *Documents and archival records*
  Documents and archived records provide valuable objective data, which complement the more subjective sources of information. Examples are procedures, security policies and reports on security breaches.
- *Direct observation*
  Observation can also strengthen evidence of the case study. It is a valuable source of evidence, which complements both interviews and documents. Direct observation gives insight on how, for example, mitigating measures against the insider threat are applied in practice.

6.2. Selection of cases

A multiple case study is an analysis of the same or similar situations in different organizations. The number of available cases is limited, because of the confidentiality of the topic of information security. But, as with the literature review, quality is more important than quantity. Cases that are included form a cross-section of organizations, which vary over the type of information they use for their operations (i.e. intellectual property, medical information and financial data). Three cases are included:

- *Public institution;* This non-profit organization processes financial data and personal information of all citizens of the Netherlands.
- *Care institute;* This organization makes use of highly confidential medical information of patients that needs to be continuously available.
- *Chemical company;* this company operates in a highly competitive market and therefore wants to protect its valuable information (intellectual property).

6.3. Propositions

The literature review resulted in the conceptual model described in section 4. To gain insights in the use of the concepts in practice, the concepts are translated into interview questions.

1. **Respondent**
   - What is your function and/or responsibility within the organization?
   - What is your role in relation to the topic of information security?
   - Are you familiar with the insider threat problem?

2. **Organization**
    - What is the main product or service that the organization delivers?
    - In what kind of market does the organization operate (i.e. competitive, non-profit)?
    - What is the primary goal or mission of the organization?
    - Is the security of information assets considered to be an important business process?
    - Who is responsible for the security of information assets? Is it the responsibility of one specific person (i.e. Security Officer)?
    - Does the organization need to comply with legislation or regulation on the topic of information security?

3. **Valuation of information assets**
    - What users make use of information and/or information systems?
    - What kind of information is considered valuable to the organization?
    - In what manner is this information stored (i.e. hardcopy, information system)?
    - What are the requirements for the security of these valuable information assets? Requirements on the confidentiality, integrity or availability?

4. **Threats to confidentiality, integrity and availability of information**
    - To what kind of threats are the valuable information assets exposed?
    - Did you identify these threats by applying a risk assessment? Is this risk assessment applied on a regular basis?
    - Is the insider threat considered to be a critical threat to the identified information assets?
    - Are then any examples of insider security incidents? What was the impact of these incidents?

5. **Measures to mitigate insider threats**
    - What is the general risk minimization strategy of the organization?
    - What kind of measures are taken, including formal-, informal- and technical measures, to mitigate insider threats (section 5.3)?
    - What was the point of departure for the implementation of the measures (i.e. risk assessment)?
    - In what manners are these measures implemented (i.e. security education, communication)?
    - What is the performance of these measures to mitigate insider threats?
    - What are the vulnerabilities of the implemented measures?

6.4. Protocol

The application of a case study protocol is an important factor in safeguarding the validity of the case studies. The internal validity of the case studies is improved by applying a standard questionnaire, based on the propositions mentioned above, which makes it possible to compare the three cases. The concepts that are used in the questionnaire are derived from the literature review.

The external validity of the case studies is increased by the selection of cases that form a cross-section of organizations that vary over the type of information they value, the requirements to the confidentiality, integrity and availability of this information, and the type of market in which the organization operates (i.e. non-profit, competitive market).

6.5. Results

This section describes the course of the interviews. The interviews were the main sources of evidence for the case studies and were held with key members of the three organizations that had knowledge about the security of information (Table 13). For the public institution and the care institute this resulted in both cases in an interview with representatives of the IT department. The interviews took approximately 1.5 hour. The focus was on the identification of measures that the organizations had taken to mitigate threats to information that they considered valuable and/or critical.

The interviews at the public institution and the care institute were based on a standard research protocol that included the interview questions stated in section 6.4. The interview questions were sent one week before the actual interview was held and interview results were reviewed by the respondents before publication in this report.

Case study	Interview date	Details	Additional information
Public institution	24-11-‘08	1 interview with a representative of the IT department	Guideline for Information Security; Security Infrastructure documentation; Website;
Care institute	27-11-‘08	1 interview with 2 representatives of the IT department	Guideline for Information Security; General statistics on IT Infrastructure; Report on Information Security at Care institute by the Netherlands Health Care Inspectorate; Website;
Chemical company	18-12-’08 to 23-01-‘09	7 interviews (phase 1) with representatives of the key business processes; 3 interviews (phase 2) with representatives of the IT department	Draft Security policy; Business Continuity Plan; Risk assessment; Website;

Table 13: Overview of case study interviews

The case studies at the public institution and care institute acted as a reference point for the extensive case study held at the chemical company. The case study at the chemical company was held at a more detailed level and included multiple interviews in which the different business processes were represented (Table 13). The duration of the interviews varied from 30 minutes to 2.5 hour and focused on the identification of valuable information, the identification of locations in which this valuable information is stored, the possible threats to the confidentiality of the information and the measures to mitigate these threats. Members of the information management department were consulted to complete the identification of current measures and vulnerabilities.

The multiple case studies resulted not only in insight in the application of security measures in practice, but also in the strengths and weaknesses (e.g. vulnerabilities) of those measures. In addition, the interviews gave an impression of the general awareness on the topic of information security and more specifically on the topic of insider threats. Although the number of interviews at the public institution and the care institute were limited, the internal validity was increased by the use of additional acquired information (e.g. security documentation). The results of the case studies are described in section 7.

7. Description of case study results

In section 6.4 the concepts in the conceptual model were translated into propositions that were used as interview questions for the three case studies. This section describes the results of the case studies and answers the research questions by gathering data from practice. Sections 7.1 to 7.3 give a summary of the most important research findings for each of the cases. An extensive description of the case study results is included in Appendix D. Section 7.4 gives a general overview of the application of the measures that were described in section 5.2.

7.1. Case study – Public Institution

The public institution serves around 7 million clients, including both private persons and businesses. The institution processes financial- and private information of all of its clients, which results in financial transactions in which several billions of euro's are involved. The institution focuses especially on the integrity of information. The internal ICT organization consists of 3500 staff members, including approximately 500 externals from preferred partners. 50 members of the ICT organization are engaged in information security.

The public institution is aware of the importance of information security and acknowledges the possible threat that can be caused by insiders. The responsibility of the information security process is, however, not appointed to a single person; there is no information security officer. There is a guideline for information security that describes security norms and according measures. The guideline needs improvements such as a classification of information assets and accompanying handling policies. In addition, it should be noted that the norms and measures that are described in the guideline are not derived from a risk assessment. The public institution has implemented many of the measures found in literature (section 5.2). Some of them need minor improvements and/or need to be applied more consistently to decrease the number of vulnerabilities. In Appendix D – 1 more details on the strengths and weaknesses of the applied measures are described.

7.2. Case study – Care Institute

The care institute includes three hospitals and three policlinics in which a total of 6000 employees work either full time or part time. There are 2500 workplaces available, which make use of approximately 300 applications (including the Hospital Information System and Picture Archiving and Communication Systems - PACS). The IT department is responsible for the implementation of information security measures. These include not only virus protection, but also implementation of NEN7510 (Best practice for information security in hospitals) and security awareness practices. The focus of the information security process is on the availability and confidentiality of information (i.e. patient information, strategic information). It should be noted, however, that the quality of health care takes precedence over the security of the information that is involved.

Although the care institute acknowledges the possible threats that insiders can pose, it thinks that the occurrence of these threats is not very likely: most of the end users in the hospitals (e.g. clinicians) are very honorable and have signed special code of conducts that deal with the secrecy of patient information. The care institute has implemented many of the measures found in literature (section 5.2). It is clear that some of the measures cannot be applied strictly, due to the specific characteristics of the open environment of hospitals and the possibility of emergency situations in which patients' lives could be at stake. In Appendix D – 2 more details on the strengths and weaknesses of the applied measures are described.

7.3. Case study – Chemical Company

The chemical company uses a patented process to produce products that operate in highly competitive markets. To ensure the continuity of the primary production process, but also the secondary business processes, the company makes use of a variety of information systems. These information systems include strategic information, financial information but also intellectual property that give the organization a competitive advantage. The IT department, consisting of approximately 20 members, is responsible for the implementation of security measures. The focus is on the confidentiality of information.

Although the chemical company acknowledges the potential threats that insiders could pose to the confidentiality of information, it has not performed a risk assessment to identify these threats. The information security process is not embedded in the organization and therefore there is no insight in the actual threats to information security. The chemical company has implemented a number of measures of which some need improvements. These improvements vary from more strict application of measures to a more regular check for compliance. In Appendix D – 3 more details on the strengths and weaknesses of the applied measures are described.

7.4. Application of measures in case studies

This section gives an overview of the measures that are applied in the three case studies. Table 14 represents a summary of these measures. The list of measures is derived from section 5.2. Some measures are applied correctly and others need (minor) improvements. In some of the cases measures were applied incorrectly. Table 14 also shows some recommended measures that are derived from the measures that were described in section 5.2.

It can be concluded that, of the three case studies, the public institution applied most of the measures that were described in literature correctly. There are only two measures that are additionally recommended: watermarking and data loss prevention suites. These two measures were, however, also lacking at the two other case studies. Some key concerns for all three case studies are:

- Lack of a security policy
  The security policy of the public institution is based on a set of norms and accompanying measures, which is in fact a good start. However, the policy does not include a classification of information assets and handling policies. The security policy of the chemical company is in draft. The care institute does only have guidelines for appropriate use of computer facilities (e.g. email use) and needs to develop a corporate security policy.
- Compliance of the clean desk policy
  Although there is a clean desk policy present in all three case studies, the policy is not applied consistently and compliance is not regularly checked.
- Lack of an incident registration
  The public institution and the care institute described the process of registering security incidents; however, in practice this registration is not kept. The chemical company does not register security incidents. Incident registration is recommended to be able to recognize trends in for example misuse of applications.
- Application of security education
  The care institute is planning and preparing for the application of security education in the near future. The public institution creates security awareness through the communication of guidelines to managers that are involved. Like the chemical company, the public institution did not, however, apply security education and training.

- Lack of monitoring and logging, and audits.
  The chemical company does not apply monitoring and logging (including Intrusion Detection Systems) to its primary information systems. This also results in restricted possibilities of auditing the effectiveness of applied procedures and/or end user actions. The public institution does not apply monitoring and logging consistently and the care institute applies it only when there is a suspicion of misuse.

An overview of the measures that were applied in practice (Table 14):

	Case studies		
Measures	Public institution	Care institute	Chemical company
Security policy	⚠	✗	✗
Pre-employment screening	✓	✓	✓
Third party contracts	✓	✓	⚠
Legally binding documents	✓	✓	✓
Physical access control	✓	⚠	⚠
Dual control	✓	✓	✗
Separation of duties	✓	✓	✓
Least privilege	✓	⚠	✗
Revocation authorizations	✓	✓	⚠
Clean desk policy	⚠	⚠	⚠
Restrictions remov. media	✓	✓	✚
Contingency planning	✓	✓	✓
Audit	⚠	⚠	✗
Security in SDLC	✓	n/a	n/a
Incident registration	✗	✗	✚
Security education	⚠	⚠	✚
Manage org. culture	✓	✓	✓
Clear screen policy	✓	✚	✓
Authentication	✓	⚠	✓
Role Based Access Control	✓	✓	✗
Antivirus	✓	✓	✓
Encryption	⚠	⚠	⚠
Watermarking	✚	✚	✚
Monitoring and logging	⚠	⚠	✚
Intrusion Detection Systems	⚠	✚	✚
Data Loss Prevention suites	✚	✚	✚
Backup	✓	✓	✓
Application controls	✓	✓	✓

Legend:
✓ - Measure is applied correctly
⚠ - Measure needs improvements
✗ - Measure is not applied correctly
✚ - Additional recommended measure

Table 14: Overview of measures applied in case studies

An extensive analysis of the three case studies, including a comparison and a case specific analysis, is described in section 8.

8. Analysis of case studies

This section describes the analysis of the three case studies described in section 7. The section starts with a cross-case analysis, section 8.1, which describes a mutual comparison of the case studies. In section 8.2 a within-case analysis is performed, to gain insight in the issues that specifically apply to the specific cases.

8.1. Cross-case analysis

This section describes the comparison of the three case studies described in section 7. The comparison starts with the identification of a security profile that determines the focus of the information security process. The comparison then continues in section 8.1.2 with an evaluation of the maturity of the information security process. Section 8.1.3 identifies the differences between the application of the information security process in practice compared to the literature.

8.1.1. Security profile

The security profile describes the focus on the organizations' security efforts (see section 3.1.1). It is determined by the primary mission, goals and process of an organization. Information security is concerned with the confidentiality, integrity and availability of information. Organizations need to make concessions in addressing these security properties, they may need to focus on availability and put less effort in addressing confidentiality. The interests of different parties involved, can thus result in conflicting security focuses.

Figure 11 represents the security profile of the three case studies described in section 7.

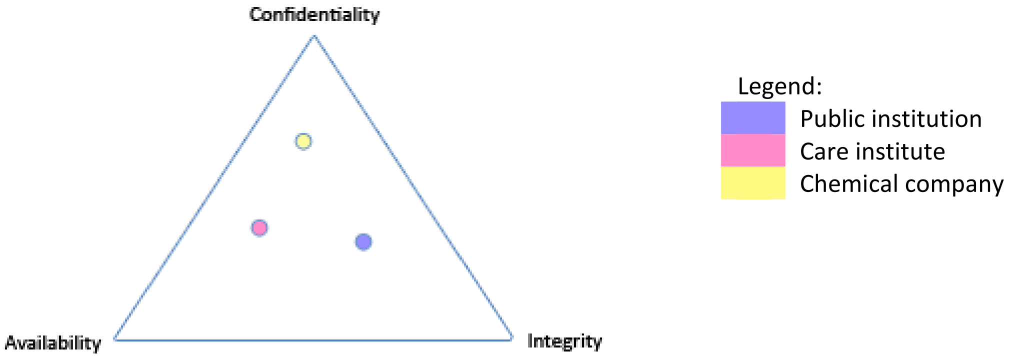


Figure 11: Information security profile of case studies

The security profile of the public institution is mainly focused on the protection of the integrity of the information. This is the result of the fact that the organization processes financial- and private information of around 7 million clients that result in financial transactions in which several billions of euro's are involved. The focus of the care institute, due to the mission to guarantee an optimal quality of health care, is mainly on the availability aspect of their information. The confidentiality and integrity of patient information are, however, also important. The security profile of the chemical company is focused on protecting the confidentiality of information that gives the organization a competitive advantage.

Because the security profile represents the focus on security efforts, based on an organizations' primary mission and goals, it is the point of departure for a risk assessment and risk minimization strategy.

8.1.2. Information security maturity

Information security maturity modeling is based on a method of evaluating the organization in different levels. Although information security management standards and checklists have received a lot of attention, little research has been done to study the existing information security management-oriented maturity models (Siponen, 2002). Siponen (2002) therefore analyzed the available information security maturity models from the point of view of software engineering literature. The most 'mature' information security maturity model is the one proposed by Stacey (1996), the information security program maturity grid. This approach is derived from the maturity model that the Software Engineering Institute defined for the maturity of software development capability, the Capability Maturity Model (CMM).

The maturity grid by Stacey (1996) proposes five stages in order of increased maturity:

- **Stage 1 – Uncertainty.** A total lack of understanding of information security, security is a hindrance to productivity.
- **Stage 2 – Awakening.** Realization of the value of security, but inability to provide resources and money for security.
- **Stage 3 – Enlightenment.** Security is a must, as well as resources and money for security, organizations need also to prevent violation, instead of merely recovering from incidents.
- **Stage 4 – Wisdom.** Security developments reflects organizations' environmental factors and needs, all users are empowered in terms of information security.
- **Stage 5 – Benevolence.** Continuous security process improvement through research and practice.

More detailed prescriptions associated with each maturity level are incorporated in Appendix E, which also includes detailed steps to improve the stages of maturity. Each of the stages can be applied to five categories that evaluate information security efforts: Management understanding and attitude, security organization status, incident handling, security economics and security improvement actions.

The maturity model of Stacey can be used to identify the actual performance of the organizational information security process, compare the current status to other organizations in the industry and can set targets for the improvement of the information security process. Especially in the case of information security and due to all the outsourcing occurring, the advantage of being able to compare levels of maturity between different organizations is attractive. Siponen (2002) states that the key promise of information security maturity models is that if organizations want to do business with, or otherwise co-operate with, other organizations, there is a need to ensure that those organizations do not constitute the weakest security link in their systems.

More detailed prescriptions associated with each maturity level are incorporated in Appendix E, which also includes detailed steps to improve the stages of maturity. Each of the stages can be applied to five categories that evaluate information security efforts.

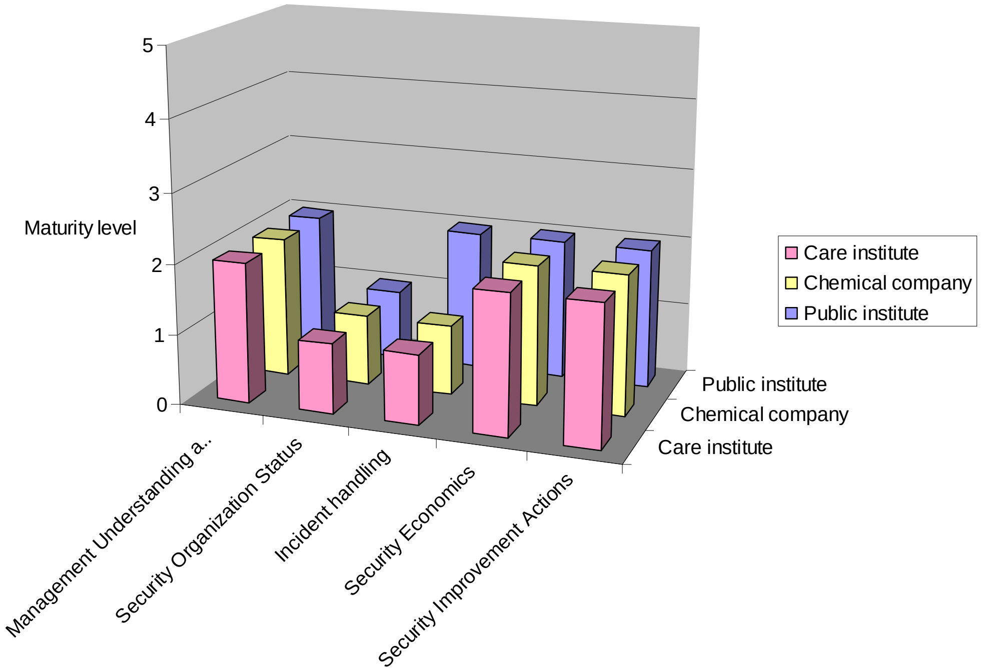


Figure 12: Graphical representation of information security maturity of case studies

Figure 12 shows the application of the maturity model and represents the maturity levels of the information security process of the three case studies described in section 7. The maturity level is determined by evaluating the steps that correspond with the maturity levels for each of the five categories, included in Appendix E. The maturity levels of the three case studies are on a comparable level, except for the fact that the public institute handles incidents in a more mature way. Although the public institute has implemented more of the measures that were found in literature, compared to the other two cases, their overall information security maturity level is on a comparable level. In each of the three cases management realizes that information security may be of value, however, an information security officer is not in all cases appointed. The expenditures on security measures are in none of the cases based on a proper risk analysis (e.g. the care institute describes a risk assessment, but did not apply it up to now). In addition, there is no security awareness created through security training and communication of enterprise wide security policies.

The desirable maturity level of organizations lies at the maturity level of 4, because this level represents an organization that is in control of its information security process. There is thus room for improvement for each of the three case studies. These improvements are based on the steps that are described in Appendix E and are discussed in section 9. However, section 8.1.3 first continues with a discussion on the differences between theory and practice.

8.1.3. Theory versus practice

The three case studies show some interesting differences between the application of information security in theory and in practice. First of all, theory and best practices claim that the point of departure for the application of information security is a proper risk assessment (section 5.4). This risk assessment identifies the possible threats and vulnerabilities and makes it possible to choose a risk minimization strategy to mitigate these threats and vulnerabilities. In practice, however, organizations tend to apply measures without proper evaluation of risks to their valuable information.

Theory extensively describes possible threats originating both from the inside and outside. It could be valuable for organizations to consider these threats as a point of departure for the risk assessment. In practice, more attention is thus given to the implementation of measures, without knowing the actual risks that need to be mitigated. The three organizations did however apply all three types of measures, including formal, informal and technical measures.

The three case studies also reveal that data on insider threat occurrences is not readily available. As was stated in theory, available data on insider threat occurrence is limited. All three cases could not give insight in the number of security incidents caused by insiders with for example malicious intents. Therefore it would be likely that most insider attacks remain undetected when they occur (section 3.4).

8.2. Within-case analysis

This section describes the within-case analysis of the three case studies described in section 7. The within-case analysis is focused on the identification of vulnerabilities that exist due to absence and/or gaps in the efficiency of mitigating measures. The within-case analysis is the input for the case study advices that are described in section 9.

8.2.1. Public institution

Based on the case study description some potential vulnerabilities to the confidentiality, integrity and availability of information of the public institution can be identified:

- The public institution is not aware of the actual threats to the confidentiality, integrity and availability of information because it did not apply a proper risk assessment to identify possible threats.
- The guidelines for information security do not describe the classification of information assets and therefore accompanying handling policies cannot be applied. Valuable information should be treated accordingly. The guideline is communicated through responsible managers, but compliance is not checked.
- The responsibility for the information security process is not formally established.
- Although there is a clean desk policy, this measure is not applied consistently. Compliance is not regularly checked.
- The registration of security incidents is not applied correctly. Trends to security incidents, and specifically insider incidents, cannot be recognized. Although the information security guidelines prescribe the registration, analysis and response to security incidents, it is not applied in practice.
- Although monitoring and logging tools, including Intrusion Detection Systems, are available these loggings are only randomly checked or in cases of exceptions. It is, however, unlikely that these exceptions will be identified by for example watchful employees, because there is no sense of security awareness created through security education.
- Although general audits can be carried out, audits on the number of security incidents and the efficiency of current measures cannot be carried out because of the lack of data.
- Encryption is correctly applied on laptops to prevent disclosure of information. Use of USB sticks is only allowed for members of the ICT organization. These USB devices are however not encrypted. This could result in disclosure of information.

8.2.2. Care institute

Based on the case study description some potential vulnerabilities to the confidentiality, integrity and availability of information of the care institute can be identified:

- The care institute is not aware of the actual threats to the confidentiality, integrity and availability of information because it did not apply a proper risk assessment to identify possible threats.
- There are no guidelines on information security. The use of IT facilities is documented and communicated to new employees. The guidelines that govern behavior and describe the efforts of the organization to control damage by threats are, however, not present.
- The responsibility for the information security process is not formally established.
- Physical access control is weak because of the open environment of hospitals. Some critical facilities, such as the emergency room, server rooms and offices of staff personal are however restricted to authorized users.
- The principle of least privilege cannot be applied properly in the hospital environment. Every authenticated clinician can see any patient’s data; excessive restrictions on authorizations can directly result in loss of patients’ lives.
- Although there is a clean desk policy, this measure is not applied consistently. Medical documents are left unattended in rooms to which outsiders (i.e. insiders without need-to-know, visitors) can gain access.
- The registration of security incidents is not applied. Trends to security incidents, and specifically insider incidents, cannot be recognized. Although it is claimed that incidents are registered, the care institute could not demonstrate the effectiveness of the measure by showing reports of security incidents.
- Employees are informed about guidelines for the use of IT facilities when they are hired. Currently, however, there is no security education and/or training applied to create security awareness and commitment.
- Although monitoring and logging is possible in the Citrix environment, it is not applied unless there is a well-founded suspicion of misuse. Audits on misuse of insiders are therefore not readily available. Monitoring and logging helps to identify the perpetrator, therefore it is hard to prosecute malicious insiders when monitoring and logging is not applied.

8.2.3. Chemical company

Based on the case study description some potential vulnerabilities to the confidentiality, integrity and availability of information of the care institute can be identified:

- The chemical company is not aware of the actual threats to the confidentiality, integrity and availability of information because it did not apply a proper risk assessment to identify possible threats. Up to now there is only a risk assessment applied that evaluates threats to the availability of information.
- The security policy is in draft and not communicated throughout the organization, there is also no security awareness created through the application of security education.
- There is no classification of information assets and accompanying handling policies are not set. The distribution and/or transportation of confidential information is therefore not restricted (e.g. hardcopy, removable media).
- Confidential information is shared with third parties, although third party contracts include secrecy agreements, there is no actual control on the distribution of this information by third party companies to, for example, competitors. Collaboration with third parties is based on contracts, but above all, trust.

- Administrators have extensive rights on servers, databases and data to be able to perform their duties. However, there is no actual control on what actions were carried out and there is no measure implemented to assure that not one single administrator could carry out actions with major impacts information security. The principle of dual control is not applied correctly.
- The principle of least privilege is not applied consistently. End-users have extensive rights to not only view, but also download, confidential business information. This makes it possible to distribute large amounts of information using network access. In addition, there is no monitoring and logging applied to identify misuse. Monitoring and logging helps to identify the perpetrator, therefore it is hard to prosecute malicious insiders when monitoring and logging is not applied.
- Although access to critical applications is based on Role Based Access Control, end-users have possibilities to exploit their authorized access to disclose confidential information. In addition, there is no control on access to shares on the network.
- Physical access control is weak because of the fact that buildings are located on industrial parks that give access to a variety of firms. Although there is authentication needed to enter buildings, offices are not locked. In addition, the clean desk policy is not applied consistently. Access to information that was left unattended can be attained easily.
- Although the clean desk policy is communicated throughout the organization, there is no actual control on compliance. This results in offices in which confidential information can actually be found left unattended.
- Revocation of authorizations is based on reports of account inactivity of 100 days and a monthly HR report of job terminations; an insider can thus abuse his user account after job termination without going noticed until the end of the month. Revocation of authorizations after job changes is not applied.

The results of the insider threat assessment of the case study at the chemical company are extensively described in Appendix A.

9. Case study recommendations

This section describes the case study advice that is based on the identification of potential vulnerabilities described in section 8.2 and the measures to mitigate threats that are described in section 5. Table 12 in section 5.3 shows to what degree the measures that were found in literature mitigate the possible insider threats. Based on the degree of mitigation these measures can be prioritized.

The case study advices in section 9.1, 9.2 and 9.3 include not only measures to address possible insider threats but also measures to increase the overall security maturity level of the organization.

9.1. Public institution

Compared to the other two cases, the public institution applies more of the measures that were suggested by literature. The overall security maturity level is, however, comparable to the other case studies. This contradiction shows that the application of measures at the public institution does not imply that the overall information security process is mature. The application of measures should be based on a proper risk assessment and analysis, which gives insight in the threats to which the organization is exposed. Because of the focus of the public institution towards integrity of information, special attention to threats that result in modification of information should be given.

The task of determining the security policy, creating security awareness and embedding the information security process should be delegated to an information security officer, that is supported by management. Currently there is no single person responsible for the process of information security. Management needs to understand that information security is an essential part of an organizations´ internal control. The security policy should define and govern the actions and behaviors of insiders. It includes a description of the measures that are applied, prescribes correct handling of information and sets the consequences for offences. To support the security policy, and to enhance compliance, security awareness through training and clear procedures should be created.

Security awareness can also increase alertness towards potential indicators (i.e. deliberate markers, verbal behavior) of malicious activities. In addition, more attention should be given to the registration of security incidents that relate to insider misuse. In this manner, trends can be recognized and impacts of malicious activities can be timely reduced.

The public institution has the tools to apply monitoring and logging. Because the public institution already possesses the tools, it is advised to apply regular analysis of loggings. The loggings are, however, only checked randomly and in exceptional cases. One of the problems of addressing insider threats is the fact that insiders have legitimate access to information and thus nothing exceptional happens. Anomaly based detection, which is searching for abnormal use of for example information, can however detect misuse of this category. The public institution has an intrusion detection system at its disposal, so detection of exceptional use should be possible. It should be noted, however, that the power to detect malicious insiders is very limited unless the system is specifically designed for insider threat detection.

To be able to address threats to the confidentiality of the information used, the public institution should consistently apply a clean desk policy. In addition, encryption should be applied to prevent disclosure of confidential business information stored on USB devices and other removable media.

9.2. Care institute

Like the public institution and the chemical company, the care institute does not have insight in the actual threats to the security of their valuable information. It is therefore strongly advisable to apply a proper risk analysis, which focuses especially on threats to the availability and confidentiality of valuable information (e.g. patient information). The case study confirms, however, that special requirements for the selection of appropriate measures need to be applied.

Because a patients' life can depend on the availability of information, it is for example hard to implement the principle of least privilege: all clinicians need access to medical records of the patient. Therefore physical access to computers and information systems need to restricted for patients and visitors. In addition, the care institute should reconsider the application of a clear screen policy for computers that are not directly used in emergency facilities (i.e. emergency room, intensive care). To create commitment and compliance, security education is needed. Part of the security education should be the communication of guidelines for appropriate use of information, consequences for offences and security efforts that are described in a corporate security policy.

There is a general feeling of trust towards employees and third party contractors. There is however no incident registration process that could prove the opposite. It would be advisable to register incidents to be able to recognize trends in possible insider misuse. In addition, monitoring and logging is only applied in cases of a well-founded suspicion of misuse. Due to the fact that there is no security awareness created, it is unlikely that monitoring and logging will actually be applied, because insiders are not trained to recognize potential indicators of misuse. It is therefore advisable to regularly apply the tools that are readily available to be able to detect possible misuse.

Especially in the case of the care institute, watermarking and data loss prevention suites would be useful tools to detect distribution of, for example, medical records. Watermarking adds (digital) data to the documents, data loss prevention suites are able to track data in motion (e.g. email gateway filters), data at rest (e.g. hosts that scan shares) and data in use (e.g. monitoring removable media).

9.3. Chemical company

Due to the fact that the chemical company operates in a highly competitive market, the focus of the application of information security measures should be on the confidentiality of information. It is advisable to delegate the responsibility to a corporate security officer which attains management support. The security officer then needs to gain insights in the actual threats and vulnerabilities to which the organization is exposed, in order to select appropriate measures. This insight can be gained by applying a proper risk assessment. Once appropriate measures have been selected and applied, the security officer needs to set up a security policy.

Although there is already a draft version of the security policy, the content is not supported by management. In general, it is therefore advisable to create security awareness at both management and end-users. Security education and training facilitates awareness. Part of the security education is the communication of security policies. An important aspect of this security policy is a classification of information assets. This classification should result in information that is labelled and handled in accordance, which prevents unintentional disclosure.

Another measure that can be advised, is the application of restrictions on the use of removable media. Information that is labelled as high confidential should for example be prohibited to be stored on USB devices. By applying data loss prevention suites that track the use of files, compliance of these measures can be controlled. When the chemical company decides to accept the use of USB devices, it is strongly advised to apply encryption in order to prevent for disclosure when the USB device is lost. Encryption is advisable, even if high confidential information is prohibited.

The chemical company shares also information with third parties (e.g. engineering companies) that are for example responsible for the creation and modification of technical drawings of machinery. Although third party contracts are applied, it is advisable to be careful with the selection of such third parties. Additional background information should be attained, including. for example, periodic reports and/or audits on the application of security measures.

To protect information from disclosure by insiders, improvements need to be made to the application of the principle of least privilege. Both administrators and end-users have extensive access rights to applications that store large amounts of confidential information. Large numbers of end-users are not only able to view this information, but are also able to download and distribute it. To gain insight in the use of this information, monitoring and logging needs to be enabled. By regularly reviewing these loggings, misuse can be detected timely.

An extensive advice to the chemical company is described in Appendix A.

10. Conclusions

"Security is just like air. It is originally worthless,
but its existence will not be painfully detected until it is lost".
(Kwo-Jean Farn)

This section describes the conclusions and recommendations that can be derived from both the literature review and multiple case studies. Section 10.1 starts with an overview of general conclusions, section 10.2 continues with a reflection on the research problem and research questions. Section 10.3 includes suggestions for further research, which are based on the limitations of this research.

10.1. General conclusions

This section describes the overall conclusions that can be derived from both the literature review and the multiple case studies. The overall conclusions are listed below:

- **Scientific literature on insider threat problem is not yet mature**

Based on the literature review in section 2 it can be concluded that the maturity of available scientific literature on the insider threat problem is low. Most of the available research that was found was conceptual and confirms the remarks of Schultz (2002) that few empirical studies of insider attacks are publicly available to guide approaches to the insider threat problem. Defining the problem boundaries is hard, not least because of the lack of appropriate definitions and contextual information, but also because of the lack of data for analysis, experimentation and, ultimately, validation of proposed solutions (section 2.2). The little existing available literature consists thus of non-validated models that are mostly presented in conference papers. In general the number of papers on the topic of information security in the leading IS journals has diminished (section 2.2). The few models of and studies about insider attacks and related issues that are available in scientific literature are a good start, but they are of little value in producing meaningful results that can help organizations reduce the frequency of and damage from insider attacks (section 2.2).

- **Limited insight in effectiveness of measures**

The lack of available data on insider incidents causes limited insight in the effectiveness of measures. According to literature this lack of data is driven by a variety of factors, the most prominent of which appears to be the sensitivity of the topic: organizations that have been the victims of insider attacks tend to handle such (known) incidents as quietly as possible (section 2.2). The multiple case studies show, however, that organizations are not even aware of the insider threat problem (section 8.1.3). Based on this lack of security awareness, the absence of incident registration and monitoring and logging, it can be concluded that organizations are perhaps not even capable of giving insight in the effectiveness of applied measures. There is thus hardly any empirical evidence of the effectiveness of measures. In addition, the application of measures is very context-dependent. Evaluation of the effectiveness of measures may be subjective and stakeholder specific.

Although there is limited insight in the effectiveness of measures, it is clear that current practices are inadequate for dealing effectively with insider threats. It is particularly revealing that this opinion is shared by many experienced security practitioners in the financial services industry, a sector that has both had considerable experience with malicious insiders and is a very aggressive adopter of new security technologies and practices (section 5.4). It is suggested that successful defense against insider threats depends on both technical and behavioral solutions, which include formal-, informal- and technical measures (section 5.1.1). It remains hard, however, to reduce the threats posed by insiders that misuse their authorized access to information. Better screening, security awareness and fine-grained access control could reduce these threats. There are, however, costs to such measures. These costs include financial expenditures on IT resources, reductions of productivity and creativity, and an erosion of trust between employer and employees (section 5.5).

- **Gap between measures described in literature and applied in practice**

The multiple case studies show a gap between the measures that were found in literature (extensively described in Appendix B) and the application of measures in practice. The gap is the result of the absence of measures or the limited efficiency of applied measures. For various reasons, organizations have difficulties to implement measures in practice. There is always a balance between measures and applicability. The care institute, like many medical institutions, allows for example every authenticated clinician to see any patient's data; in their experience, limiting access to 'need-to-know' is too complex, and erring on the side of excessive restriction can directly result in loss of patients' lives. In other cases, however, the gap is the result of a general lack of security awareness.

- **Reduction is the main risk minimization strategy**

Organizations can choose between different risk minimization strategies (section 3.4.4). All three case study organizations have applied the reduction or mitigation strategy, which confirms the assumption (section 3.4.4) that this is the primary risk minimization strategy used in practice. In addition, the case study organizations have also accepted some of risks as a cost of doing business. However, the latter seems to be the result of a general lack of security awareness and insight in actual threats to the security of information.

- **Overall maturity level of case study organizations is low**

The information security program maturity grid (section 8.1.2), is a method for evaluating the actual performance of the organizational information security process, compare the current status to other organizations in the industry and to set targets for the improvement of the information security process. The evaluation of the three case studies revealed that on the basis of five categories, none of the organizations had a maturity level that was higher than 2. In each of the three cases management realizes that information security may be of value, however, an information security officer is not in all cases appointed. The expenditures on security measures are in neither of the cases based on a proper risk analysis. In addition, there is no security awareness created through security training and communication of enterprise wide security policies.

It is also striking that, although the public institute has implemented more of measures that were found in literature, compared to the other two cases, their overall information security maturity level is on a comparable level (section 8.1.2). This implicates that the implementation of measures does not directly mean that the overall maturity level will raise. A desirable maturity level for an organization would be maturity level 4, because this level reflects an organization that is in control of its information security process. To improve the general maturity level, it is important to embed information security in the organization, through the creation of commitment and awareness (section 9).

- **Case study organizations are not aware of actual threats**

Theory and best practices claim that the point of departure for the application of information security measures is a proper risk assessment. This risk assessment identifies the possible threats and vulnerabilities and makes it possible to choose a risk minimization strategy to mitigate these threats and vulnerabilities. The three case study organizations, however, tend to apply measures without proper evaluation of risks to their valuable information. These organizations are not aware of the actual threats to which they are exposed. More attention is given to the implementation of measures, be it without knowing the actual threats that need to be mitigated (section 8.1.3).

- **General feeling of trust towards insiders**

It is good to know that most insiders can actually be trusted, it cannot be ruled out however, that misuse of information, either deliberately or accidentally, occurs. Although the three case study organizations realize that misuse of information occurs, a general feeling of trust towards insiders prevails (section 7). They simply assume that deliberate misuse is negligible and should be accounted for as a residual risk.

10.2. Reflection on research problem and questions

This section reflects the research problem from both the perspective of the literature review and the perspective of the multiple case study. In section 1.1 the research problem is stated:

What can firms, the chemical company in particular, do to protect their information against the insider threat problem?

In section 8 specific advices for each of the case studies were given. In each of the cases the point of departure for the implementation of information security measures is the application of a proper risk assessment. The risk assessment identifies possible threats and vulnerabilities to the confidentiality, integrity and availability of information. Based on these threats and vulnerabilities, resulting from either the absence of measures or gaps in efficiency of applied measures, organizations need to choose appropriate risk minimization strategies. The implementation of information security measures should thus be based on identified threats and vulnerabilities. Formal-, informal- and technical measures need to complement each other, to successfully reduce the threats posed by insiders. However, as was stated before, it is clear that current practices are inadequate for dealing effectively with insider attacks.

It is advisable to prevent the occurrence of insider threats by applying better screening, creating organization-wide security awareness and enhancing control on access to valuable information. In addition, monitoring and logging can be applied to identify the perpetrator closely after the attack. There are, however, costs to such measures. These include not only financially related costs, but also (and probably most important) an erosion of trust between employer and employees.

Answering the research problem and the research objective was supported by three additional research questions:

I. **What is the insider threat problem?**
II. **What possible solutions and mitigating measures, both theoretical and practical, exist to address the insider threat problem?**
III. **What are the strengths and weaknesses of mitigating measures in addressing the insider threat problem?**

The first question gave insight in the characteristics of the insider threat problem, and was addressed in section 3. The second question gave insight in the measures that were proposed in literature and the application of these measures in practice. This research question was addressed in section 5, 7 and 8. The third question could, however, only be partly addressed. There is hardly any empirical evidence on the effectiveness of measures in scientific literature (section 2.2) and the multiple case studies could only give limited insight in the strengths and weaknesses of the application of measures in practice (section 8).

10.3.Suggestions for further research

- This master thesis describes both measures that were found in literature and measures that were applied in practice. Although assumptions were made on the efficiency of those measures, based on the identified vulnerabilities in practice and scientific literature, there is no validated evidence of the efficiency of security measures. According to some of the conference papers that were reviewed, this was caused by the lack of available data on insider threats. It is therefore suggested to gain more insight in the available insider attack cases through better cooperation with the business world.
- The lack of data on insider threats results also in a large number of non-validated conceptual models. It is therefore suggested that more effort is placed in gaining insight in for example insider attack cases.
- Because of the globalization and the increasing interdependency between organizations it is suggested that more research is needed on the topic of determining the security maturity level of organizations. One standard for determining these levels would mean that organization can select third parties on a maturity level that meets their standards. Although this topic seems to be of value, and security best practices already exist, not much progress has currently been made (Siponen, 2002).

11. References

Albert, C., Dorofee, A. (2001). *Octave Threat profiles*. Pittsburgh, PA: Software Engineering Institute. Carnegie Mellon University.

Andersen, D.F. et al. (2004). *Preliminary System Dynamics Maps of the Insider Cyber-threat Problem*. In Twenty Second International Conference of the System Dynamics Society. Oxford, UK, pp. 1-36.

Anderson, J.P. (1980). *Computer security threat monitoring and surveillance*. Technical report, James P. Anderson Co., Fort Washington, PA.

Anderson, R.H. et al. (2000). *Research on mitigating the insider threat to information systems*. In Proceedings of a Workshop Held August 2000.

Baker, W.H., Hylender, C.D. & Valentine, J.A. (2008). *2008 Data Breach Investigations Report.* Obtained from www.verizonbusiness.com, October 2008.

Bellovin, S.M. (2008). *The Insider Attack Problem Nature and Scope.* In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 1-4.

Bishop, M. (2005). *Panel: The Insider Problem Revisited.* In Proceedings of the 2005 workshop on New security paradigms (Lake Arrowhead, USA), pp. 75-76.

Bojanc, R., Jerman-Blazic, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management 28*, pp. 413-422.

Brackney, R.C., Anderson, R.H. (2004). *Understanding the Insider Threat.* In Proceedings of a March 2004 Workshop (March 2-4, 2004, Rockville, MD, USA).

Butts, J.W., Mills, R.F. & Baldwin, R.O. (2005). *Developing an Insider Threat Model Using Functional Decomposition.* In Proceedings of the Third international workshop on mathematical methods, models, and architectures for computer network security (St. Petersburg, Russia, September 25-27), pp. 412-417.

Capelli, D., Moore, A., Shimeall, T.J., Trzeciak, R. (2006). *Common Sense Guide to Prevention and Detection of Insider Threats*. Obtained from http://www.cert.org/insider_threat/, Octobre 2008.

Capelli, D., Moore, A., Shimeall, T.J., Trzeciak, R. (2009). *Common Sense Guide to Prevention and Detection of Insider Threats v3*. Obtained from http://www.cert.org/insider_threat/, January 2009.

Carroll, M.D. (2006). *Information Security: Examing and Managing the insider Threat.* In Proceedings of the 3rd annual conference on Information security curriculum development, Kennesaw, Georgia (USA).

Caruso, V.L. (2003). *Outsourcing Information Technology and The Insider Threat.* Master Thesis, Air Force Institute of Technology (Wright-Patterson Air Force Base, Ohio).

Daft, R.L. (2000). *Management.* Harcourt College Publishers, Orlando, USA. 5th edition, pp. 670.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security 7 (4),* pp. 171/175.

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security 20 (2)*, pp.165-172.

Dhillon, G., Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security 20 (8),* pp.715-723.

Ezingeard, J. N., Mcfadzean, E., & Birchall, D. (2005). A model of Information Assurance Benefits. *Information Systems Management 22 (2),* pp. 20-29.

Furnell, S.M., Phyo, A.H. (2003). Considering the Problem of Insider IT Misuse. *Australian Journal of Information Systems 10 (2),* pp. 134-138.

Furnell, S.M., Phyo, A.H. (2004). *A detection-oriented classification of insider it misuse*, in Third Security Conference, April 2004.

Franqueira, V.N.L., van Eck, P.A.T. (2006). *Defense against insider threat: a framework for gathering goal-based requirements*, http://eprints.eemcs.utwente.nl/9615/, Enschede, Technical Report TRCTIT-06-75. Obtained: Octobre 2008.

Greitzer, F.L. et al. (2008). Combating the Insider Cyber Threat, *IEEE Security and Privacy 6 (1),* pp. 61-64.

Hannah, D.R. (2006). Keeping Trade Secrets Secret. *MIT Sloan Management Review 47 (3),* pp. 17-20.

Hunker, J. (2008). *Taking Stock and Looking Forward – An Outsider's Perspective on the Insider Threat.* In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 195-213.

ISO/IEC 15408 (1999). Information technology — Security techniques — Evaluation criteria for IT security. ISO/IEC Switzerland.

Keromytis, (2008). *Hard Problems and Research Challenges Concluding Remarks.* In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 215-218.

Magklaras, G.B., Furnell, S.M. (2002). Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Computers & Security 21 (1),* pp. 62-73.

Martinez-Moyano, I. J. et al. (2008). A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach*. ACM Transactions on Modeling and Computer Simulations 18 (2),* pp. 7-34.

McMormick, M. (2008). *Data Theft: A Prototypical Insider Threat*. In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 53-68.

Melara, C. et al. (2003). *A System Dynamics Model of an Insider Attack on an Information System.* In Proceedings of the 21st International Conference of the System Dynamics Society (New York, USA, July 20-24).

National Institute of Standards and Technology Special Publications 800-30: Risk Management Guide (DRAFT), June 2001.

Neumann, P.G. (1999). *The challenges of Insider Misuse*. SRI Computer Science Laboratory, Paper prepared for the Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse, 16-18 August 1999, at RAND, Santa Monica, CA.

Overbeek, P., Lindgreen, E.R., Spruit, M. (2002). *Informatiebeveiliging onder controle*, Amsterdam: Pearsons Education.

Pare, G. (2004). Investigating Information Systems with positivist case study research, *Communications of the Association for Information Systems 13*, pp. 233-264.

Pleeger, C.P. (2008). *Reflections on the Insider Threat*. In Insider Attack and Cyber Security, Beyond the hacker, pp. 5-15.

Predd, J. et al. (2008). Insider Behaving Badly. *IEEE Security and Privacy 6 (4),* pp. 66-70.

Richardson, R. (2008). 2008 CSI Computer Crime & Security Survey. Obtained from www.gocsi.com

Schwartz, R.B., Russo, M.C. (2004). How to Quickly Find Articles in the Top IS Journals. *Communications of the ACM 47 (2)*, pp. 98-101.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security 21 (6),* pp. 526-531.

Schutzer, D. (2008). *Research challenges for fighting insider threat in the financial services industry.* In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 215-218.

Sinclair, S., Smith, S.W. (2008*). Preventative Directions for Insider Threat Mitigation Via Access Control*. In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 165-193.

Siponen, M.T. (2002). Towards Maturity of Information Security Maturity Criteria: Six lessons learned from software maturity criteria. *Information Management & Computer Security 10 (5),* pp. 337-436.

Siponen, M.T., Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions, *ACM SIGMIS Database 38 (1),* pp. 60-80.

Siponen, M., Willison, R. (2007). *A Critical Assessment of IS Security Research between 1990-2004.* In proceedings of 15th European Conference on Information Systems, Switzerland, St. Gallen.

Stacey, T.R. (1996). Information security program maturity grid. *Information Systems Security 5 (2).*

Tuglular, T. (2000). A Preliminary Structural Approach to Insider Computer Misuse Incidents. *EICAR 2000 Best Paper Proceedings*, pp.105 -125.

Vadera et al. (2008). 2008 Information Security Breaches Survey. *Technical Report.*

Wood, B. (2000). *An Insider Threat Model for Adversary Simulation.* In proceedings of the conference on Research on Mitigating the Insider Threat to Information Systems #2 (Arlington, USA), Appendix B, pp. 41-48.

Appendix A – Extensive case study Chemical Company

Due to the sensitivity of the topic, Appendix A is considered confidential and therefore not included in the public version of the master thesis. Below follows a description of the methods used.

The results of the extensive case study at the chemical company are reported in a separate document. The extensive case study included an insider threat analysis. The insider threat analysis is based on generic risk analysis practices. The approach results in the typical steps of identifying critical information assets, potential threats and current measures and vulnerabilities, that are needed to determine the risk of insider threat occurrence. The analysis results in a prioritized list of recommended measures to mitigate the risk of insider threats. A schematic representation of the structure of the analysis is shown in Figure 13.

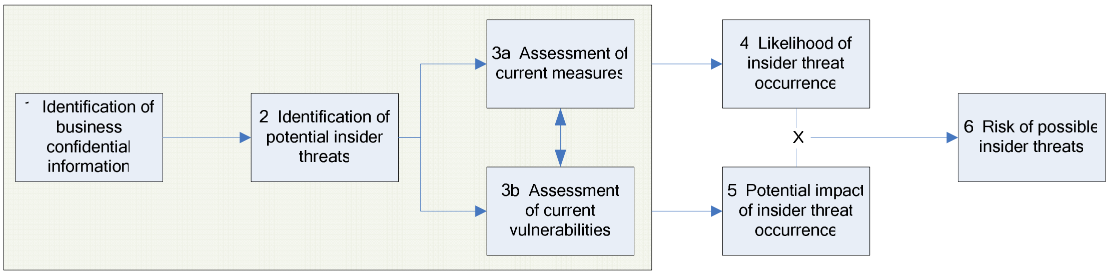

1 Identification of business confidential information
2 Identification of potential insider threats
3a Assessment of current measures
3b Assessment of current vulnerabilities
4 Likelihood of insider threat occurrence
X
5 Potential impact of insider threat occurrence
6 Risk of possible insider threats

Figure 13: Schematic representation of the insider threat analysis

1. Identification of business confidential information

This step describes the identification of business confidential information that is derived from interviews with key members of the organization. The information that can be considered business confidential includes strategic information, financial information, operational information and intellectual property.

2. Identification of potential insider threats

The potential threats to business confidential information are derived from the Insider threat profiles described in section 3.3. Due to the scope of the case study at the chemical company, the identification of potential insider threats is restricted to threats that could result in disclosure of information.

3. Assessment of current measures and related vulnerabilities

In this step current measures are identified and evaluated. In addition, the related vulnerabilities are also described. The identification of these measures is based on the categorization of mitigating measures described in section 5.2. The identified measures were evaluated on their degree of efficiency (Table 15).

Legend:

Measure applied correctly	✓
Measure needs improvements	⚠
Measure is not applied correctly	✗
Additional recommended measure	+

Table 15: Degree of efficiency of current measures

4. Likelihood of insider threat occurrence

Based on the results of the first three steps, the likelihood of insider threat occurrence can be determined (or calculated). The likelihood of threat occurrence is the probability that an insider poses a threat by exploiting vulnerabilities. Threats are likely to happen in part because there is motivation, either intentional or unintentional, but also because there are vulnerabilities which provide opportunities. These vulnerabilities could result from the absence of mitigating measures or gaps in the efficiency of applied measures.

The likelihood of threat occurrence can be derived from the degree of efficiency of applied measures (Table 12, section 5.3 – low, medium and high mitigation) and the actual status of the applied measures (Table 15). In Table 16 grades were given to both the degree of efficiency of measures and the current status of application:

	Measure applied correctly	Measure applied, needs improvements	Measure not applied (correctly)
Low mitigation	1	2	4
Medium mitigation	2	4	8
High mitigation	4	8	16

Table 16: Calculation of likelihood of threat occurrence

In case a measure with high efficiency has not been applied, the score will be high. The higher the overall score for a specific threat (e.g. measures that mitigate the threat are not applied or need improvements), the higher the opportunity for a motivated insider to pose a threat. In this manner, the threats with the highest opportunity for an insider of the chemical company can be put in order. It should be noted however, that for a threat to occur, there also needs to be a (malicious) insider that exploits this opportunity.

5. Potential impact of threat occurrence

During the survey the respondents were also asked to value the degree of confidentiality of the information assets that were identified. The information assets that were identified in step 1 were all considered business confidential. However, some assets are considered to have a higher classification of confidentiality than others, because they represent higher impacts when disclosed.

6. Risk of possible insider threats

The risk of possible insider threats is the product of the likelihood of threat occurrence and the impact of threat occurrence. In table 17 the threats are ordered in accordance with their likelihood of occurrence and the information assets are grouped in accordance with their degree of confidentiality (impact).

The items in the top left corner of table 17 represent the information assets that have the highest risk to run in threats to confidentiality. Based on this schematic view on the actual risks to the confidentiality of information, the chemical company can choose to apply risk minimization strategies.

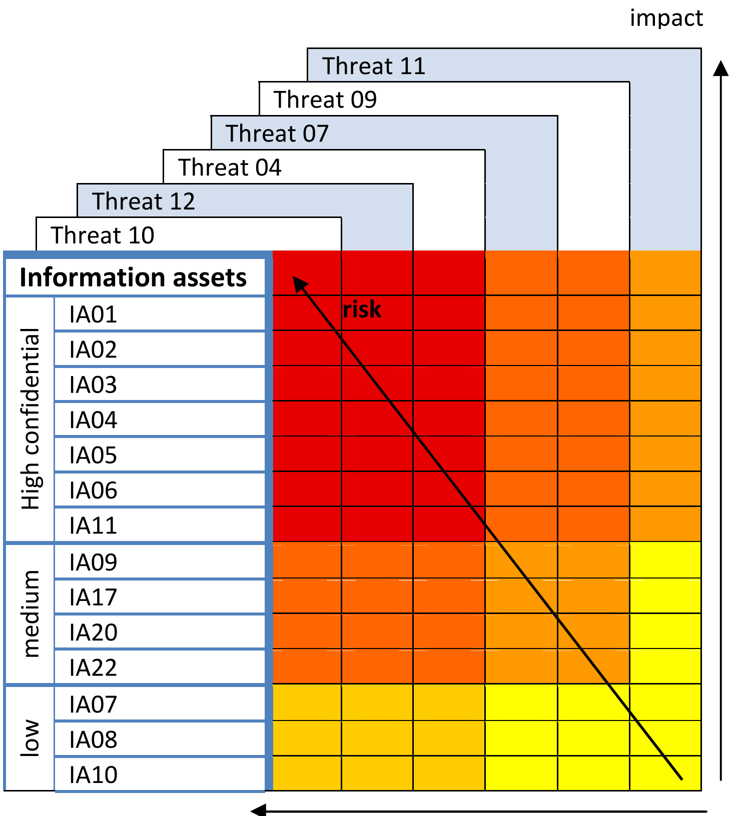


Table 17: Risk of possible insider threats

Appendix B – Literature review results and synthesis

This appendix extensively describes the results of the literature review that was carried out in accordance with section 2. Appendix B-1 includes the results of the systematic literature review and Appendix B-2 includes the synthesis of the literature on the insider threat problem.

B – 1. Systematic literature review

The systematic literature review described in section 2 can be schematically represented by Figure 14. The figure shows that the papers that were found were evaluated based on their title and abstract. After this rough selection, the remaining papers were read. This resulted in exclusion of more papers. The resulting papers were compared and synthesized (Appendix B - 2). As a result of reading these papers, additional papers were included for review (e.g. bottom-up searching).

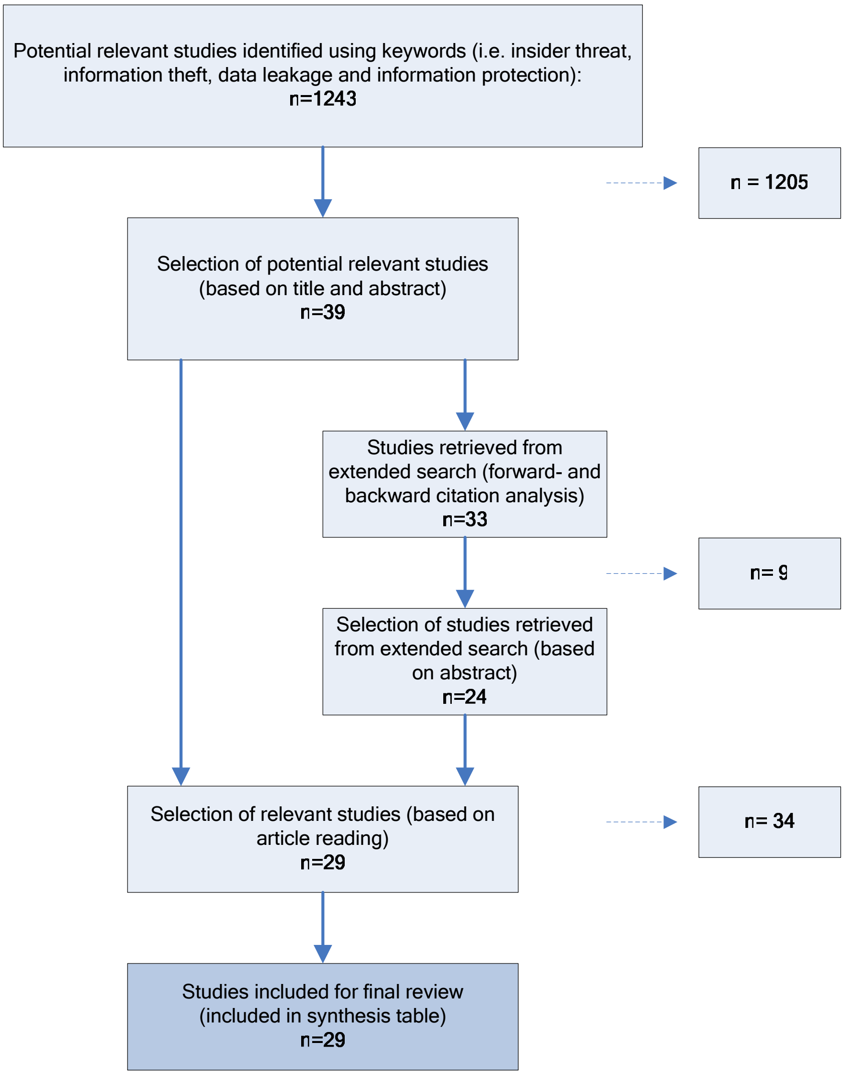

Potential relevant studies identified using keywords (i.e. insider threat, information theft, data leakage and information protection):
n=1243
n = 1205
Selection of potential relevant studies (based on title and abstract)
n=39
Studies retrieved from extended search (forward- and backward citation analysis)
n=33
n= 9
Selection of studies retrieved from extended search (based on abstract)
n=24
Selection of relevant studies (based on article reading)
n=29
n= 34
Studies included for final review (included in synthesis table)
n=29

Figure 14: Results of systematic literature review

B – 2. Literature synthesis

The systematic literature review resulted in 29 useful scientific papers that describe (in part) the insider threat problem. Forward and backward citation analysis resulted in (conference) papers that were not found using the initial keywords in Scopus. Table 15 synthesizes the papers that were found, based on the concepts that were addressed, the focus and the research method that was used.

	Concepts																			Focus	Research method
	Insiders					*Noncompliant insiders*					*Insider threats*			*Mitigating / Counter measures*							
Reference	Trusted	Access	Knowledge	Skills	Security Perimeter	Motivation	Risk	Tactics	Process	Actions	Fraud	IT Sabotage	Espionage	Prevention	Detection	Responding	Technical	Formal	Informal		
Andersen et al. (2004)											x	x	x				x	x		Insider threat model	Case study
Anderson (1980)		x								x				x	x		x	x		Insider action classification	Conceptual
Anderson et al. (2001)														x	x		x			Insider threat models and measures	Conceptual
Bellovin (2008)														x	x		x	x		Insider attacks and defence/detection	Conceptual
Bishop (2005)			x		x						x	x	x							Definition of insider threat	Conceptual
Brackney & Anderson (2004)		x								x	x	x	x							Insider actions taxonomy	Conceptual
Butts, et al. (2005)	x									x	x	x	x							Decomposition of insider actions	Conceptual
Capelli, et al. (2006)											x	x	x	x	x		x	x	x	Best practice prevent/detect threat	Case study
Capelli et al. (2009)											x	x	x	x	x		x	x	x	Best practice prevent/detect threat	Case study
Carroll (2006)						x								x	x	x				Insider threat framework	Conceptual
Dhillon (1999)																	x	x	x	Mitigation of insider threats	Case study
Dhillon (2001)														x	x			x		Measures to prevent insider threat	Case study
Dhillon & Moores (2001)														x	x		x	x		Measures to address insider threat	Case study
Furnell & Phyo (2003)											x	x	x	x	x		x	x		Insider threat and measures	Conceptual
Furnell & Phyo (2004)										x					x					Detection-based insider threat model	Conceptual

	Concepts																			Focus	Research method
	Insiders					*Noncompliant insiders*					*Insider threats*			*Mitigating / Counter measures*							
Reference	Trusted	Access	Knowledge	Skills	Security Perimeter	Motivation	Risk	Tactics	Process	Actions	Fraud	IT Sabotage	Espionage	Prevention	Detection	Responding	Technical	Formal	Informal		
Franqueira & van Eck (2006)	x	x	x			x				x	x	x	x	x	x		x	x	x	Defense against insider threats	Conceptual
Hannah (2006)													x	x				x		Measures to prevent espionage	Conceptual
Keromytis (2008)	x	x	x											x	x		x	x	x	Problems and Research challenges	Conceptual
Magklaras & Furnell (2002)			x		x	x					x	x	x	x						Insider threat prevention	Conceptual
Martinez et al. (2008)											x			x	x			x		Awareness training	Non-reactive
Melara et al. (2003)											x	x	x	x	x		x	x		Modeling the insider threat	Non-reactive
Neumann (1999)		x	x		x									x	x	x				Defense against insider misuse	Conceptual
Pfleeger (2008)		x				x									x		x			Reflections on insider threat	Conceptual
Predd, et al. (2008)	x					x					x	x	x							Taxonomy insider actions	Conceptual
Schultz (2002)	x				x				x					x	x					Indicators of insider attack	Conceptual
Schutzer (2008)														x			x	x		Measures to prevent insider attacks	Conceptual
Sinclair & Smith (2008)		x															x	x		Mitigation through access control	Conceptual
Tuglular (2000)						x								x	x					Insider misuse framework	Conceptual
Wood (2000)		x	x	x		x	x	x	x		x	x	x							Modeling the insider threat	Conceptual

Table 18: Synthesis of literature on the insider threat problem

Appendix C – Measures to address insider threats

The measures that are mentioned in Table 11 (see subsection 5.2) are extensively described below. The section is divided into subsections in accordance with the categorization by Dhillon (1999).

C – 1. Formal measures

Formal measures include business structures and processes that ensure the correct general conduct of business and reduce the probability of an incident or an attack, or at least minimize its impact (see section 5). The formal measures that are able to address the insider threat problem are described below.

F01 – Security policy

The security policy defines and governs actions and behaviours of personnel within an organization. Internal policy is the base for regulatory compliance and insider incident prevention (Carroll, 2006). The security policy includes the organizations efforts to control damage by threats, both originating from the inside and outside, identified in the risk assessment. Corporate security policies may attempt to prescribe correct handling of sensitive information, however, policies that are not supported by clear procedures, training and tools are generally doomed to be ineffective or disregarded (McMormick, 2008).

F02 – Pre-employment screening

Screening of prospective new insiders, including new employees, contractors and temps before hiring them could dramatically reduce the likelihood of insider threats. Studies (Schutzer, 2008) have shown that approximately 1/3 of all convicted insiders had prior arrests. Although privacy concerns have to be addressed, enquiring former employers and asking for certificates of good conduct can be a good starting point.

F03 – Third party contracts

It is important to set information security requirements in third party contracts to ensure that information and information systems are used in compliance with the organization’s security policy. In addition, such contracts can require compliance to regulations that proof security maturity. Third party contracts are an important measure to address the problem of misuse by hired insiders.

F04 – Legally binding documents

To prevent loss or theft of business confidential information, and especially intellectual property, organizations can require insiders (i.e. employees, contractors, visitors, temps) to sign agreements that (Hannah, 2006):

- Prohibit insiders from using or disclosing business confidential information of the organization (non-disclosure-agreement)
- Restrict the companies, geographic areas and industries in which insiders can work following the termination of their employment (non-compete-agreement)
- Give up all legal rights to the organization to new inventions, ideas or products developed in the course of their employment (assignment provisions)

F05 – Physical access control

Physical access control should ensure that only persons with legitimate access can enter facilities and buildings. Appropriate access control is based on proper identification (T02) of persons. Physical access control must be applied explicitly to critical facilities (i.e. power supply, server rooms).

F06 – Dual control

The principle of dual control (also called two-person rule or four-eye principle) requires two individuals, usually with identical roles and hierarchical position, to perform sensitive tasks (Franqueira and van Eck, 2006). By applying the principle of dual control a single insider cannot perform a sensitive task that could have a major impact on confidentiality, integrity or availability of information.

F07 – Separation of duties

Separation of duties ensures that no single user is permitted or technically able to release changes. This prevents that a single (malicious) user can perform a task that could have major impact on confidentiality, integrity or availability of information. This principle can be difficult to achieve in small organizations (Franqueira and van Eck, 2006). Separation of duties should be taken into consideration when applying Role Based Access Control (T03).

F08 – Least privilege and need-to-know

The principle of least privilege is based on the assumption that insiders only need to be assigned to the minimum set of privileges needed to perform their duties. Need-to-know is a special case of least privilege that is for example used in military environments. It relies on labels for individuals and objects to restrict access to information (Franqueira and van Eck, 2006). The principle should be taken into consideration when applying Role Based Access Control (T03).

F09 – Revocation of authorizations

Revocation of authorizations is concerned with the change or deletion of authorizations after job rotations or retirement of insiders. Insider threat studies (Capelli et al, 2006) show that many former employees posed threats using non-revoked user accounts and authorizations. Therefore the revocation of authorization is an important measure to prevent insider (i.e. former employees) misuse.

F10 – Clean desk policy

Securely storing business confidential information reduces the likelihood of theft by insiders. Information that is valuable to the organization should not be left unattended on desks in rooms that are open for insiders like visitors, colleagues or other persons with legitimate access (i.e. service technicians, janitors). Not only hardcopies should be protected, but also removable media like CDs and USB devices deserve special attention.

F11 – Restrictions on use of removable media

Removable media makes it possible to store an enormous amount of valuable information on a device that can be easily transported out of the organization. Because of the relative ease of use and the advances in mobility, organizations tend to forget the security risks resulting from for example the loss of such removable media devices. Therefore the use of removable media should be restricted to prevent loss or disclosure of valuable information. Another possibility to mitigate this risk is to encrypt the removable media devices (T05) or to use port lockdown products that disable USB, CD and floppy ports (McMormick, 2008).

F12 – Contingency planning

Contingency planning is a measure to minimize the interruptions caused by successful insider security breaches. Contingency planning is concerned with effective backup (see T10) and recovery processes and is therefore specifically related to threats to the integrity and availability of information.

F13 – Audit

Auditing refers to the examination and verification of various network, system, and application logs or data. To prevent or detect insider threats, it is important that auditing involves the review and verification of changes to *any* of the organization's critical assets. Furthermore, auditing must examine and verify the integrity as well as the legitimacy of logged access (Capelli et al., 2009). It should be ensured that audit data cannot be modified by anyone in the organization.

F14 – Security in Software Development Life Cycle (SDLC)

Security, including possible insider threats, should be taken into consideration during the software development life cycle (SDLC). Insiders that are involved in the SDLC could take advantage of defects, resulting from insertion of malicious code or logic bombs. In addition, insiders that have recognized the vulnerabilities could also use them to carry out fraudulent activities.

F15 – Incident registration

The registration of incidents is important to be able to recognize trends in incidents that could be related to insiders. These incidents could be related to issues concerning security violations (i.e. malicious insider activities, accidental errors).

C – 2. Informal measures

Informal measures deal with the culture, value and belief system of an organization (section 5.1.1). The informal measures that are able to address the insider threat problem are described below.

I01 – Security education

Increasing security awareness is the most cost-effective control that an organization can apply (Dhillon, 1999; Hannah, 2006). Security education facilitates awareness. Insiders must understand that security policies and procedures exist, that there is a good reason for them to exist, that insiders need to comply with them and that serious consequences exist for infractions (Capelli et al., 2006). In addition members of the organization should be educated to watch for exceptional behavior such as deliberate markers, meaningful errors and verbal behavior (Schultz, 2002). Security education is important to effectively implement security policies, but cannot deter intentionally wrongful behavior among malicious employees.

I02 – Manage organizational culture

It is important to manage the organizational culture and to show management commitment towards employees. An organizational culture in which it is possible to understand management' s intentions, and which is conducive to developing a shared vision and other informal objectives, would make members of the organization more committed to their activities and to the success of the organization as a whole (Melara et al., 2003). Because there is a feeling of trust, employees are more likely to share feelings of dissatisfaction or other negative workplace issues. The latter deserves special attention because research (Capelli et al., 2009) shows that disgruntled employees are responsible for the majority of insider attacks.

C – 3. Technical measures

Technical measures include mechanisms to protect information stored in information systems from attacks or incidents (section 5.1.1). The technical measures that are able to address the insider threat problem are described below.

T01 – Clear screen policy
In addition to clean desks (F10), the clear screen policy should prevent unauthorized persons from obtaining authorized access to systems via a computer that was left unattended. The clear screen policy can be applied by implementing password protected screensavers.

T02 – Authentication
Authentication is an important defense layer in mitigating the insider threat. Authentication is concerned with verification and determines if an insider is in fact the person he or she claims to be. Authentication can be applied at both the physical- and the logical security perimeter. Authentication at the physical perimeter is part of the process of physical access control (F05) and can be applied by verifying the identity of persons by reviewing their identity certificates. Authentication at the logical perimeter can be done by applying passwords, token-verification or biometrical authentication (Siponen and Oinas-Kukkonen, 2007).

T03 – Role Based Access Control (RBAC)
The basic notion of RBAC is that permissions are associated with roles, and users are assigned to appropriate roles, thereby acquiring the roles' permissions. An important part of RBAC is the implementation of the principles of least-privilege and separation of duties. The principle of least-privilege ensures that a role has only access to resources that are necessary to its legitimate, business, purpose. Separation of duties ensures that the roles' permissions for a specific business process are disseminated among multiple users. Role Based Access Control has only a limited effect on insider threats, because malicious insiders exploit legitimate access. Limiting such access may have a negative effect on non-malicious employees' productivity (Pfleeger, 2008).

T04 – Antivirus
Insiders could either deliberately or accidentally introduce malicious software that could pose a threat to the confidentiality, integrity and/or availability of valuable information. By implementing antivirus measures (i.e. antivirus and anti-spam software) installation of such malicious software could be prevented or the impact could be reduced dramatically. Insiders should also be informed about the risks of installing unknown software.

T05 – Encryption
Encryption transforms information so that it will become unreadable to a user who does not possess the knowledge, in most cases the key, to de-crypt the information. Encryption protects valuable information and is concerned with the confidentiality of information. The technique of encryption can be applied to storage devices (i.e. removable media, laptops, and mobile phones), networks (i.e. internet, wireless networks) and communication (i.e. email).

T06 – Watermarking
Digital watermarking is a technique to add either visible or invisible data to an object, including text, pictures, video or audio. The technique can be used to protect valuable information from being distributed or transported in an unauthorized manner.

T07 – Monitoring and logging
Monitoring and logging can lead to early discovery and investigation of suspicious insider actions (Capelli et al., 2009). Monitoring and logging can only be effective if account and password policies are in place, because only in that case insiders can be uniquely identified. Monitoring is the process of being aware of the activities that an insider carries out in for example an application or network, logging is the process of recording these activities. There

is controversy as to whether monitoring serves as a deterrent; that is, if insiders know their activity is being monitored are they less likely to engage in inappropriate activity. The answer to that is unknown, because of the little published research on insider attacks (Pfleeger, 2008). It should also be noted that special attention should be given to the integrity of monitoring and logging because it can be influenced by malicious insiders who have privileged access rights to these tools.

T08 – Intrusion Detection Systems (IDS)

Intrusion Detections Systems are designed to detect attacks. The working of an IDS is based on the definition of a rule set, which should be created so that all the static of employees' day-to-day work activities, such as accessing various services and servers, does not trigger attack warnings, and only the important information is reported. This important information would include detected activities that users do not require for their daily work, as well as any other glaringly obvious attacks (Einwechter in Schultz, 2002). Einwechter proposed a combination of IDSs such as Network IDSs, Host-based IDSs and Anomaly-based IDSs. Most IDSs are, however, geared towards detecting externally initiated attack patterns; other, more subtle methods are not likely to be noticed by IDSs (Schultz, 2002). This assumption is confirmed by Pfleeger (2008) who states that the hardest attack for an IDS is to recognize an attack composed of pieces spread across a long period of time. In addition, the volume of non-malicious activity far outweighs that of malicious activity. Such volume of data is hard to analyze (Pfleeger, 2008). It should be noted that the power to detect malicious insiders is thus very limited, unless the system is specifically designed for insider threat detection.

T09 – Data Loss Prevention (DLP) suites

To prevent storage or transmission of confidential information in ways that violate security or privacy policies DLP suites can be applied (McMormick, 2008). These suites include modules for data in motion (i.e. network perimeter taps, email gateway filters), data at rest (i.e. hosts that scan databases, shares, servers) and data in use (i.e. endpoint agents that monitor desktops and removable media).

T10 – Backup

Backup measures are important in assuring the availability of valuable information. Insider threats, including for example sabotage or theft of information, could result in loss or destruction of information. Backup measures should be taken to recover the valuable information. Separation of duties should assure that no single person is responsible for the complete backup process.

T11 – Application controls

Application controls are performed automatically by information systems. Application controls are designed to ensure the complete and accurate processing of data, from input through output. Application controls include for example authentication and authorization checks (see T02), but also validity checks that ensure the input of valid data. Application controls could prevent both deliberate and accidental threats posed by insiders.

Appendix D – Extensive description of case study results

D – 1. Case study – Public institution

This section describes the case study of a public institution in the Netherlands. The section describes a small introduction of the organization, the identification of valuable information and the need to safeguard this information, the insider threat problem and measures that are taken to mitigate this threat.

D – 1.1. Introduction

The public institution serves around 7 million clients, including both private persons and businesses. The public institution processes financial- and private information of all of its clients, and deals with political, policy and legal rules, both at European and at national level. The internal ICT organization consists of approximately 3.500 staff members, including approximately 500 externals from preferred partners. It is one of the largest internal ICT organizations in the Netherlands. It advices, develops, manages and monitors the entire computer system used by the more than 30.000 staff members of the public institution. The IT infrastructure is build up out of 500 applications with multiple interfaces.

D – 1.2. Information security

The public institution processes financial- and private information of around 7 million clients that result in financial transactions in which several billions of euro's are involved. It is clear that the information that is processed must be protected: its confidentiality, integrity and availability must be assured. The institution does however focus especially on integrity. The internal ICT organization of the public institution supports this by implementing technical, formal and informal measures. 50 members of the ICT organization are engaged in information security, the responsibility for the process of information security is however not delegated to one single department in the organization: information security is part of the process of every business unit. Every business unit is responsible for making their members aware of the importance of information security.

D – 1.3. Insider threat problem

The public institution is aware of the importance of information security and acknowledges the possible threat that can be caused by insiders. Because the institution processes financial- and private information in which financial transactions are involved, they focus on integrity and confidentiality of information. But availability is also important; clients demand on time processing of information and accompanying transactions.

The integrity of employees is an issue of high importance within the public institution. The public institution does everything to prevent misuse of the financial- and private information of its clients. The results of fraud, sabotage and espionage would not only result in direct loss or disclosure of information, but would also be devastating for the image- and especially the trustworthiness of the institution.

D – 1.4. Mitigating and countermeasures

Although the ICT organization is not responsible for corporate information security, it does advice and implements measures to prevent exploitation of vulnerabilities by insider threat agents. The measures that were taken to counter the insider threat are summarized below; they are categorized into formal, informal and technical measures.

Formal measures

- *Guidelines for Information Security*
  There is one central document that describes the guideline for Information Security. The guideline is the translation of the corporate information security policy to a set of norms.

These norms are embedded in the organization and processes to assure a basic, but sufficient, security level. Every norm consists of a number of measures. The norms are not derived from a risk assessment. In addition, the guidelines for Information Security do not include a classification of information assets and accompanying handling policies. The guideline is communicated to- and accorded by responsible managers and the Management Team of the ICT organization.

- *Pre-employment screening*
  Requirements on integrity and confidentiality of insiders, both employees and externally hired personnel, are applied. These insiders have to sign a secrecy agreement and need a certificate of good conduct. Management can also decide to apply additional screening for critical functions.

- *Third party contracts*
  In case services or activities are being outsourced, the supplier needs to comply with the norms that are stated in the guideline for information security. Every outsourcing or third party contract demands a secrecy agreement, with a focus on integrity. Every contract contains arrangements on:
    - The use, transportation or publication of information
    - Logging that show when, how long, why and by whom they were carried out
    - Rules on physical access, especially outside business hours

- *Legally binding documents*
  Employee contracts do contain paragraphs that cover non-disclosure-requirements, non-compete-requirements or other statements on the confidentiality and integrity of the information that the public institution processes.

- *Physical access control*
  Access to critical facilities (secured rooms, or facilities in which confidential information is processed) is limited to employees that need to have this access for business purposes and therefore possess an access card. For both safety and security reasons it is not allowed to work without supervision. In addition, all access is registered and use of photographic-, video- or audio equipment is prohibited unless otherwise agreed upon. Third party employees may only access critical facilities when they are accompanied by an employee which is authorized to access the facility

- *Third parties and dual control*
  Remote access, to support and management information systems, is only possible through the use of connections which are explicitly designed for this purpose. In case remote access is used by third parties to carry out management operations they must be accompanied by an employee. In addition, the initiative of making connections towards third parties lies always at the ICT organization.

- *Separation of duties and least privilege*
  Separation of duties is applied throughout the organization to protect the integrity of information, data and ICT services. Functions, tasks, authorizations and responsibilities are transparently assigned on a need-to-know basis and are centrally managed in one process. The separation of duties is however not automated. End users are not allowed to mutate production information, unless these users are explicitly authorized by the data owner.

- *Revocation of authorizations*
  There is a checklist for both functional changes and retirement of personnel. Logical and physical authorizations are withdrawn at the latest on the last working day. Employees (with functions) that have direct contact with third parties need to change or circulate their functions/roles every 5 years to prevent to narrow relations with the third parties.

- *Clean desk policy*
  Although there is a clean desk policy that is part of the guidelines of information security, the policy is not applied consistently and compliance is not regularly checked.

- *Restrictions on removable media*
  The use of USB-sticks and other portable data carriers is prohibited for the end-users of the public institution, use of these data carriers is only allowed for members of the ICT organization. The USB ports in computers of the end-users are therefore disabled.

- *Contingency planning and backup*
  In the technical documentation of every ICT service is recorded which type of backup needs to be applied and what measures need to be applied in cases of emergency. This includes for example instructions on restoring backups.

- *Information security in the Software Development Life Cycle*
  It is not allowed to use production data that are reducible to confidential information (i.e. data that can be traced to natural- or legal persons) in the development and management environment. In case of exceptions that require the use of copies of production data (i.e. in the test- and acceptance environment) the data owner gives explicit written permission to make this copy. In addition, the data will be converted in a random manner. A print out of the file structure will be added to the test documentation when the test is completed, to show that every test files is deleted. For ICT-services in which outgoing money flows are involved it needs to be checked and assured that no undesirable program rules are added compared to the design. In practice these measures are, however, applied inconsistently.

- *Registration of information security incidents*
  Information security incidents, incidents on integrity and information security disturbances must be registered, analyzed, watched over and reported to the persons involved in accordance with the security guideline. This measure needs to be applied because it is important to recognize security incidents to be able to manage the risks that are involved in the deliverance of ICT services and management of data. In practice, however, the security incidents are not registered and processed accordingly.

Informal measures

- *Security education*
  Employees are informed about the rules of information security and rules on integrity both when they enter into the office and periodically. Employees are also informed through publications about rules on how to cope with threats originating from both the outside and inside.

- *Manage organizational culture*
  In every department there is a focal point to which issues on integrity (e.g. negative workplace issues) can be addressed. Overall, management shows commitment and there is a mutual feeling of trust between employees and line management.

Technical measures

- *Clear screen policy*
  A password protected screensaver is applied throughout the organization to protect PCs that are left unattended.

- *Authentication*
  Authentication at the physical perimeter is applied consistently and is based on the identification through badges. Visitors are asked to identify themselves and are escorted through buildings. Authentication at the logical perimeter is applied through username and passwords. There is no additional token verification applied.

- *Role Based Access Control*
  A major project on the application of Role Based Access Control has just been finished. Role Based Access Control is based on the principle of least privilege and need-to-know, separation of duties is also correctly applied in the assignment of roles.

- *Antivirus and Firewall*
  There is an antivirus protection installed on every workstation that includes an anti-spam and anti-phishing protection. In addition, there is an external firewall installed.

- *Removable media and encryption*
  Only 80 workplaces make use of laptops and all of them are encrypted to prevent loss of information. USB devices of the ICT organization are however not encrypted.

- *Monitoring and logging (and audits)*
  In the technical documentation of every ICT service is recorded which type of security violations need to be observed, the frequency of monitoring and the type of tooling. These security violations are automatically logged:
    - Abnormal use of functions
    - Reporting of intrusion detection or content scanning
    - Reporting of the use of vulnerable functions of data

  Security violations are logged, but only analyzed randomly. In case automatic monitoring is used, separation of duties is applied between the user that is able to mutate the security settings and the user who is responsible for analyzing and processing the observed violations. The activities of users with high system privileges are monitored, logged and randomly analyzed.

- *Intrusion Detection Systems*
  Intrusion Detection Systems (IDS) are used to detect unauthorized access to information systems and networks. It detects threats that originate from the inside and the outside. The tool monitors the 5000 employees of the ICT organization on a constant basis and is periodically used to monitor the 30.000 staff members of the public institution itself. This monitoring records approximately 30 to 40 incidents per month originating from insiders and far more from the outside.

- *Application controls*
  To prevent (accidental) misuse of applications, through for example modification, the integrity of information is improved by the implementation of application controls that restrict the actions that end-users can carry out. The determination of these controls is part of the process of security in the security development lifecycle.

D – 2. Case study – Care institute

This section describes the case study of a care institute in the Netherlands. The section describes a small introduction of the organization, the identification of valuable information and the need to safeguard this information, the insider threat problem and measures that are taken to mitigate this threat.

D – 2.1. Introduction

The care institute includes three hospitals and three policlinics in which a total of 6000 employees work either full time or part time (total of 3500 FTE). There are 2500 workplaces which make use of approximately 300 applications, including a Hospital Information System but also MS Word and MS Outlook. The organizations make use of 2000 thin clients linked to a Citrix environment, 100 PCs for PACS (Picture Archiving and Communication Systems), 350 Advanced PCs and some stand-alone and open PCs.

The care institute does not develop its own information systems; it buys licenses of existing software. The IT department assures the continuity of IT, including network, servers and information systems. The IT department is also responsible for work places, access to facilities including remote access, and incident call registration. Of the 6000 employees, 4000 have remote access to intranet and email facilities (considered as 'light accesses') and 450 make use of a more advanced remote access connection, which creates access to an environment which is equal to the work place at the care institute. In addition, there are 150 employees who make use of a smart phone (with email functionality).

D – 2.2. Information security

The IT department is also responsible for the implementation of Information Security measures. This includes protection against viruses, but also the implementation of NEN7510 (Best practice for Information Security in Hospitals) and security awareness practices. Information security is mainly focused on the availability of information systems and the confidentiality of the patient information that is stored within them. The focus is however not solely on patient information; personnel- and other critical business information (e.g. financial information) is also subject to information security measures. In general it can be stated that the quality of the health care takes precedence over the security of information that is involved. The implementation of information security measures is subject to policy and legal rules that act at a national level. The NEN7510 is a best practice to implement these legal rules and is generally accepted at the Health Care Inspectorate from the Netherlands.

D – 2.3. Insider threat problem

The care institute acknowledges the possible threats that insiders can pose, but thinks however that the occurrence of these threats is not very likely: most of the end users in the hospital environment are very honorable and in addition they have also signed a special code of conduct that deals with the secrecy of patient information. Although the likelihood might be low, there are plenty of possibilities to the loss of information resulting from insiders. The open structure of a hospital makes it hard to control what information, especially physical documents, exactly leave the perimeter. In addition, information security is fact subordinate to the care for patients which for example results in the use of group accounts in the emergency department.

D – 2.4. Mitigating and countermeasures

The measures that were taken to counter the insider threat are summarized below; they are categorized into formal, informal and technical measures. The objective of the care institute is to offer high quality health care. It is therefore that in some cases the quality of the health care takes precedence over the security of information that is involved.

Formal measures

- *Information security risk management*

  The management of risks should be embedded in the organization of the care institute. It is based on a best practice (NTA 8009-2007) on a Management system for Security for Hospitals, generally accepted in the Netherlands.

  Information security risk management is only one part of the management of risks within the care institute. Risk management within the care institute is organized in two main parts; preventive and responsive (Figure 15).

  As a result of this risk management process a risk profile of the care institute has been identified. This risk profile consists of seven primary risks; two of those risks are related to information security and possible insider threats:

  - Malfunction of ICT facilities. This will lead to local or organizational wide problems which could negatively influence or disrupt daily business.
  - Loss of data of patients, personnel and administration. This will lead to personal distress, loss of revenues and liquidity problems for the organization and its employees.

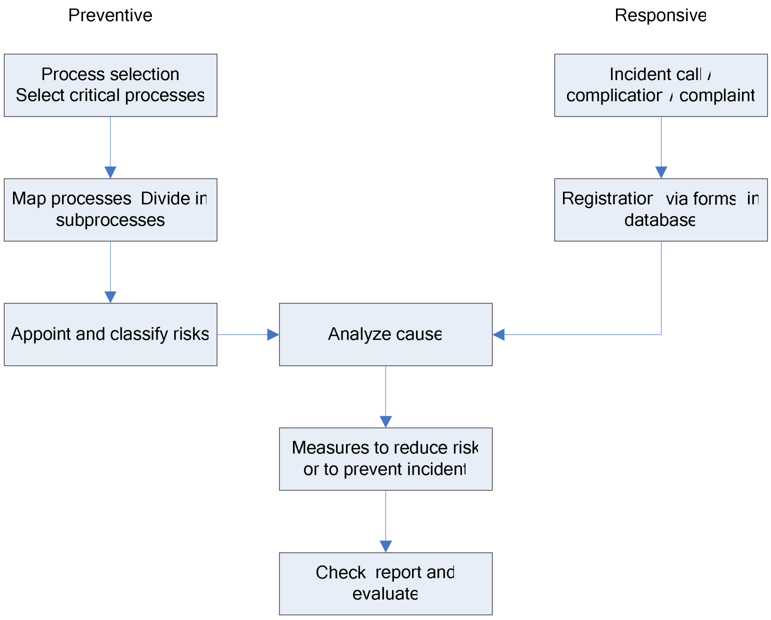


Figure 15: Risk management within the care institute (Care Institute, 2007)

  Although the risk management procedure is described extensively, it is not correctly applied in practice.

- *Guidelines for use of IT facilities*

  There is a guideline for the use of IT facilities, which includes descriptions of appropriate use of computers, remote access and email functionalities. The guideline is communicated when a new employee is hired and can be consulted via the intranet.

- *Pre-employment screening*

  Requirements on integrity and confidentiality of insiders, both employees and externally hired personnel, are applied. These insiders have to sign a secrecy agreement and need a certificate of good conduct. Management has also decided to apply additional screening for critical functions (Managers and ICT functions).

- *Third party contracts*
  Every outsourcing or third party contract demands a secrecy agreement. In addition, all the management activities are carried out in-house. Authorizations to outsourcing parties are restricted to a minimum.

- *Legally binding documents*
  Employee contracts do contain paragraphs that cover non-disclosure-requirements, non-compete-requirements or other statements on the confidentiality and integrity of the information that the public institution processes.

- *Physical access control*
  Access to critical facilities (e.g. server rooms) is limited to employees that need to have this access for business purposes and therefore possess an access card. In addition, all access is registered. Third party employees may only access critical facilities when they are accompanied by an employee which is authorized to access the facility. Because the care institute is an open environment, it is hard to control access to computers that are for example left unattented.

- *Separation of duties, least privilege and dual control*
  Separation of duties is applied throughout the organization to protect the integrity of information, data and ICT services. Authorizations are transparently assigned to functions on a need-to-know basis and are managed by the IT department. It should be noted however, that every authenticated clinician can see any patient's data; excessive restrictions on authorizations can directly result in loss of patients' lives. Every action in the Hospital Information System, which stores patient information, can be deduced to a single user. In some cases a group id is used because of usability issues.
  Both the Hospital Information System and the PACS application are based on large databases in which patient information and medical images are stored. Management of these applications and databases is in the first place the responsibility of the IT department; in case additional support is needed they will contact third parties. No one single user has full access rights to the databases mentioned, in these cases dual control is applied.

- *Revocation of authorizations*
  There is a checklist for both functional changes and retirement of personnel. Logical and physical authorizations are withdrawn at the latest on the last working day.

- *Clean desk policy*
  Although there is a clean desk policy that is part of the guidelines of information security, the policy is not applied consistently and compliance is not regularly checked.

- *Restrictions on removable media*
  The use of USB-sticks and other portable data carriers is prohibited for the end-users of the care institute, use of these data carriers is only allowed for members of the ICT organization. The USB ports in computers of the end-users are therefore disabled.

- *Contingency planning and backup*
  In the technical documentation of every ICT service is recorded which type of backup needs to be applied and what measures need to be applied in cases of emergency. This includes for example instructions on restoring backups.

- *Registration of information security incidents*
  Incidents are reported digitally and analyzed in a decentralized manner. Reported incidents include medication errors, disruptions in the phone network, malfunction of power supply or IT services. Up to now there were no incidents reported that resulted from insider threats. It did however happen that medical documents (hard copy) that contain patient data got lost.

- *Email use*
  Email use is subject to guidelines described in the general guidelines for the use of IT facilities. It is strictly prohibited to include patient information in emails, especially in emails that are addressed to outside recipients. In some cases a doctor sends information to a patient, but this only happens when a patient gives approval and is informed about the risks of sending this information over the internet.

Informal measures

- *Security education*
  Employees are informed about guidelines for the use of IT facilities when they are hired. On a short term the care institute starts with an awareness campaign to inform employees on the importance of information security.

- *Manage organizational culture*
  Most of the end users in the hospital environment are very honorable and in addition they have also signed a special code of conduct that deals with the secrecy of patient information. The organizational culture is based on mutual trust and workplace issues can be freely addressed.

Technical measures

- *Clear screen policy*
  The clear screen policy is not applied. Due to the fact that computers need to be constantly available for clinicians, application of this measures was considered to be to ‘annoying’.

- *Authentication*
  Authentication for critical facilities is applied consistently and is based on the identification through badges. Visitors are asked to identify themselves and are escorted through buildings. Authentication at the logical perimeter is applied through username and passwords. There is no additional token verification applied (except for home working).

- *Home working and authentication*
  4000 employees are able to set up a teleworking ‘light’ connection to intranet and Outlook Web Access (email) by downloading and installing a specific certificate. The certificate is linked to the IP address of their PC at the home address. The connection to the intranet and email can thus only be used at the home PC that is registered. Connecting from other places than a home situation is not allowed.
  In addition, 450 employees have a more advanced remote access connection. These employees have access to an environment which is equal to the work place at the care institute. The connection is made using a cryptocard and a secure VPN/SSL tunnel. It is not allowed to make use of this connection in an environment other than that at home. In addition, it is not possible to print or download documents.

- *Role Based Access Control*
  Access to the Hospital Information System is controlled on the basis of Role Based Access Control. It is based on the principle of least privilege and need-to-know, separation of duties is also correctly applied in the assignment of roles.

- *Antivirus and Firewall*
  There is an antivirus protection installed on every workstation that includes an anti-spam and anti-phishing protection. In addition, there is an external firewall installed. Via a proxy server, the internet traffic is routed.

- *Removable media and encryption*
  USB devices of the ICT organization are not encrypted.

- *Logging and monitoring and audits*
  The Citrix environment allows logging and monitoring of actions in a centrally managed process. However, the care institute does not monitor users on a constant basis. Activities in the Hospital Information System can however be deduced to a single person (except for some group ids that are used). The logging and monitoring is only used in cases when there is a well-founded suspicion of misuse. Logging and monitoring is thus responsive, audits on the use of the HIS are thus not applied.

- *Application controls*
  To prevent (accidental) misuse of applications, through for example modification, the integrity of information is improved by the implementation of application controls that restrict the actions that end-users can carry out.

D – 3. Case study – Chemical Company

This section describes the case study of a chemical company in the Netherlands. The section describes a small introduction of the organization, the identification of valuable information and the need to safeguard this information, the insider threat problem and measures that are taken to mitigate this threat.

The description in this section is a summary of the findings that are described in the Insider Threat report for the chemical company (Appendix A) that is kept separately due to the confidentiality of the results. This case study description will thus be on the same level of detail as appendix D – 1 and D – 2.

D – 3.1. Introduction

The chemical company uses a patented process to produce products that operate in highly competitive markets. The products are applied in a variety of end-products including tires, protective helmets and clothing, and brake pads. The organization has world wide sales offices. The production locations are, however, located in the Netherlands. The company has 1200 employees, the management of information systems and information is carried out by the IT department that includes approximately 20 members. Some of the management tasks are outsourced to third parties. The IT infrastructure is built on both physical- and virtual servers.

D – 3.2. Information security

To ensure the continuity of the primary production process, but also the secondary business processes, the chemical company makes use of a variety of information systems that contain valuable information. This valuable information includes strategic information, financial information, operational information and intellectual property that give the organization a competitive advantage. The IT department is responsible for the implementation of mitigating measures to protect the confidentiality, integrity and availability of information against threats from both the inside and outside. The process of information security is however not formally embedded in the organization. Due to the competitive market in which the company operates, the focus of information security is on the confidentiality of information.

D – 3.3. Insider threat problem

The chemical company is aware of the potential threats that insiders could pose to the confidentiality of information. Because the process of information security is not embedded in the organization, there is no insight in the actual threats to information security. Insiders have access to information that is considered highly confidential (i.e. technical drawings, intellectual property), but there is no structured approach to mitigate these threats.

D – 3.4. Mitigating and countermeasures

The measures that were taken to counter the insider threat are summarized below; they are categorized into formal, informal and technical measures.

Formal measures

- *Security policy*
  The current security policy is in draft and not communicated throughout the organization. The document includes a classification of information assets and accompanying handling policies that prescribe appropriate use of information assets. The security policy is based on the general accepted guideline for information security, the ISO/IEC 17799 Code of Information security.

- *Pre-employment screening*
  Pre-employment screening is based on risk profiles of functions and is applied correctly. For each of the functions in the organization, the risk profile is determined based on the information that is needed to be accessed for business purposes. The screening is, however, only applied to new employees and not to other insiders such as business partners, contractors and temporary employees.

- *Third party contracts*
  Security requirements are part of third party contracts, the measure is applied correctly. The focus of these security requirements is the confidentiality of information, some of the business partners are required to sign secrecy agreements.

- *Physical access control*
  Physical access control is not applied consistently; authentication before entering buildings is not applied at every location. Industrial parks results in additional vulnerabilities to unauthorized entrance of buildings. There is also no structural control on insiders that leave the security perimeter. The physical access control of critical facilities such as server rooms and production environments is, however, applied adequately.

- *Separation of duties and least privilege principle*
  The separation of duties is applied throughout the organization. Functions, tasks, authorizations and responsibilities are managed through procedures for user management. The revocation of authorizations is however not applied consistently; therefore the organization does not fully comply with the principle of least privilege.

- *Revocation of authorizations*
  Revocation of authorizations is based on reports of account inactivity of 100 days and a monthly HR report of job terminations, an insider can thus abuse his user account after job termination without going noticed until the end of the month. Revocation of authorizations after job changes (change of function or department) is not applied.

- *Clean desk policy*
  Although there is a clean desk policy that is part of the guidelines of information security, the policy is not applied consistently and compliance is not regularly checked.

- *Contingency planning*
  There is a Business Continuity Plan that describes the incident management procedure, including escalation procedures. In addition, recovery teams and detailed information on critical applications are described.

Informal measures

- *Security education*
  Employees are not regularly informed about security policies and therefore no awareness on the topic of information security is created.

- *Manage organizational culture*
  The organizational culture within the chemical company is well managed. There is management commitment and a general feeling of trust. It should be noted however that in times of economic recessions the general organizational culture could be negatively influenced.

Technical measures

- *Clear screen policy*
  The clear screen policy is applied to all computers (including laptops), except for some computers that are applied in the production process. In these cases the clear screen policy (i.e. screensaver) results in usability issues.

- *Remote access and authentication*
  Some employees are able to set up a connection to the intranet and Outlook Web Access (email) by using a token- and network verification procedure. These connections can be used in any environment with an internet connection and is used merely by sales managers. In addition, some of the employees have the possibility of working at home in an environment that is equal to that at the office. This connection is made through the use of a VPN client that requires token- and network authentication. It is possible to print and download documents to which the user is authorized. Authentication at the physical perimeter is however consistently applied. Visitors are asked to identify themselves.

- *Role Based Access Control*
  Role Based Access Control is applied correctly to information systems, but not to network shares. Users are linked to roles in applications that have authorizations restricted to those needed for business purposes. This principle is not applied to network shares and documents.

- *Antivirus and Firewall*
  There is an antivirus protection present that includes an anti-spam and anti-phishing protection. In addition, there is a firewall installed. Via a proxy server, the internet traffic is routed.

- *Encryption*
  The information that is stored on laptops is encrypted; however, the information that is stored on removable media is not. There are also no restrictions on the use of these removable media and it is therefore not prohibited to store confidential business information on these devices.

- *Backup*
  A backup scheme is followed to make backups of servers. Some of these servers are part of a cluster that is also mirrored on an external location. Backup tapes are managed by third parties.

- *Application controls*
  To prevent (accidental) misuse of applications, through for example modification, the integrity of information is improved by the implementation of application controls that restrict the actions that end-users can carry out.

Appendix E – Information Security Maturity Grid

The maturity grid by Stacey (1996) proposes five stages in order of increased maturity: Uncertainty, Awakening, Enlightenment, Wisdom and Benevolence. The tables below include detailed steps to improve the stages of maturity (Stacey, 1996). Improvements can be made on five categories that evaluate the organizations' information security efforts: Management understanding and attitude, security organization status, incident handling, security economics and security improvement actions.

	Management Understanding and Attitude
I. Uncertainty	
II. Awakening	To attain Stage II, awakening, management must approve the procurement of: ▪ The vendor-supplied, built-in software security (e.g., virus scanners, password packages, backup software, Configuration Management tools, and tape archiving tools). ▪ The vendor-supplied, built-in hardware security (e.g., equipment with high mean-timebetween-failure ratings and inventorying a high number of line-replaceable units).
III. Enlightenment	To attain Stage III, enlightenment, management must support: ▪ The enterprise wide information security policies. ▪ The information security awareness training for end-users.
IV. Wisdom	To attain Stage IV, wisdom, management must: ▪ Attend security awareness training and actually obtain an understanding of the absolutes of information security engineering, and become able to make informed policy decisions. ▪ Promote information security. ▪ Empower organizational elements to augment the enterprise's information security program consistent with the needs of the organizational element's needs.
V. Benevolence	To attain Stage V, benevolence, management must: ▪ Understand that information security engineering is an essential part of the enterprise's internal controls. ▪ Provide adequate resources and fully support the information security program to include internal research and development.

	Security Organization Status
I. Uncertainty	
II. Awakening	To attain Stage II, awakening, management must appoint an information security officer.
III. Enlightenment	To attain Stage III, enlightenment: ▪ Management must change the reporting structure of the information security officer to top management. ▪ The information security officer must develop a corporate information security policy based on the standard set of threats. ▪ The information security officer must institute a companywide information security training program. ▪ The enterprise must develop an information security strategy based on past incidents and on an analysis of the threat population and the vulnerabilities of the enterprise's assets.

	▪ Existing information security safeguards must be evaluated and augmented based on risk analyses performed in response to the standard set of threats.
IV. Wisdom	To attain Stage IV, wisdom: ▪ The information security officer must create an information security infrastructure. ▪ The information security officer must modify corporate information security policy based on a custom, enterprise-specific set of threats. ▪ Information security assessments must be updated periodically and penetration and audit capabilities must be supported. ▪ The information security officer must develop strategic alliances with other organizations (e.g., configuration management, product assurance, and procurement).
V. Benevolence	To attain Stage V, benevolence: ▪ Top management must regularly meet with the information security officer. ▪ Information security must be able to address technical problems with leading-edge solutions obtained through internal research and development. ▪ Information security's role must expand into the community to augment the enterprise's image.

	Incident Handling
I. Uncertainty	
II. Awakening	To attain Stage II, awakening: ▪ The information security officer must collect incident reports. ▪ The information security officer must respond to security incidents. ▪ Rudimentary statistics must be collected to identify major trends.
III. Enlightenment	To attain Stage III, enlightenment: ▪ The information security officer must develop a formal incident reporting procedure. ▪ Incident reports must contain the relevant data required to enable timely, proper diagnosis of the incident. ▪ Detailed statistics must be collected and analyzed to more thoroughly define the information security threat.
IV. Wisdom	To attain Stage IV, wisdom: ▪ Threats must continually be re-evaluated based on the changing threat population and on the security incidents enhancing the accuracy of the risk analyses. ▪ Legal actions must be prescribed for each type of incident.
V. Benevolence	To attain Stage V, benevolence, incident data must be analyzed and fed back continually to improve the information security process.

	Security Economics
I. Uncertainty	
II. Awakening	To attain Stage II, awakening, management must provide funding, albeit limited, for information security, allocated primarily for the procurement of safeguards supplied by vendors touting their built-in security.
III. Enlightenment	To attain Stage III, enlightenment, expenditures must be managed and justified and funding information security activities selected as a result of a risk analysis.
IV. Wisdom	To attain Stage IV, wisdom: ▪ Expenditures must be managed and continually justified through periodic risk analyses of greater accuracy, identifying additional or more cost-effective safeguards in response to the continually changing threat environment. ▪ Losses must be anticipated through cost/benefit trade-offs.
V. Benevolence	To attain Stage V, benevolence: ▪ The cost savings aspect of a completely implemented information security program must be thoroughly understood and realized. ▪ Information security expenditures must be justified and reduced, and partial funding must be obtained by information security's contribution to marketing. ▪ Information security may generate its own marketing center.

	Security Improvement Actions
I. Uncertainty	
II. Awakening	To attain Stage II, awakening, the information security officer must o implement enterprise wide security policies and procedures.
III. Enlightenment	To attain Stage III, enlightenment: ▪ The information security officer must provide a security awareness training program to encourage end-users to be more vigilant and to initiate more incident reports. ▪ Management must understand the business necessity for security. ▪ Management must fund the information security engineering activities of awareness training, risk analysis, risk-reduction initiatives, and audits.
IV. Wisdom	To attain Stage IV, wisdom: ▪ Risks must be accurately evaluated and managed. ▪ Information security engineering research activities must be initiated to keep up with the rapidly changing environment. ▪ Information security awareness must be expanded to a continuous, technical, and detailed security training program.
V. Benevolence	To attain Stage V, benevolence: ▪ The information security engineering activities (e.g., risk analyses, risk-reduction initiatives, audits, and research) must become normal, continual activities. ▪ The information security officer must obtain desirable security improvement suggestions from end-users and system owners.