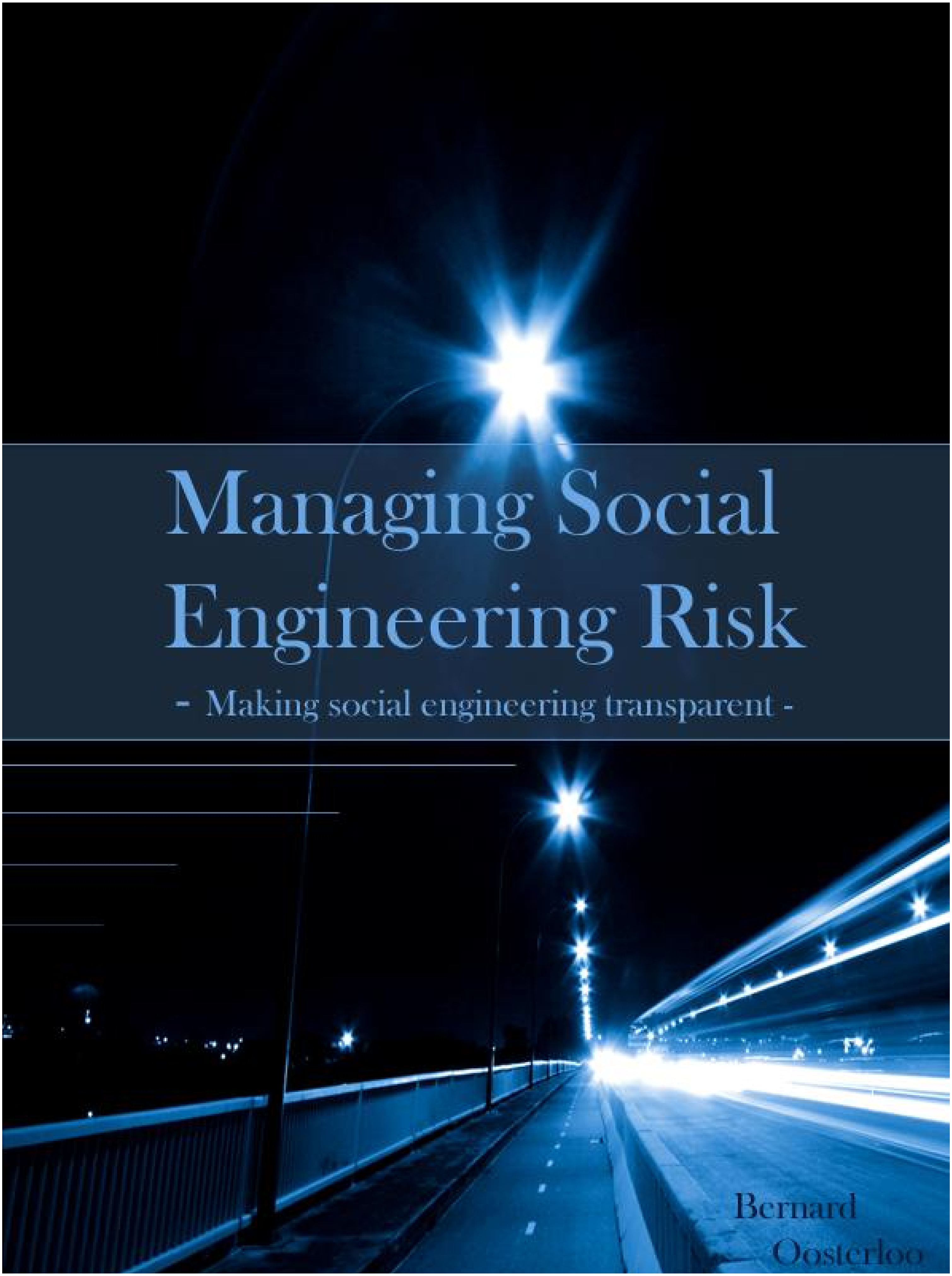
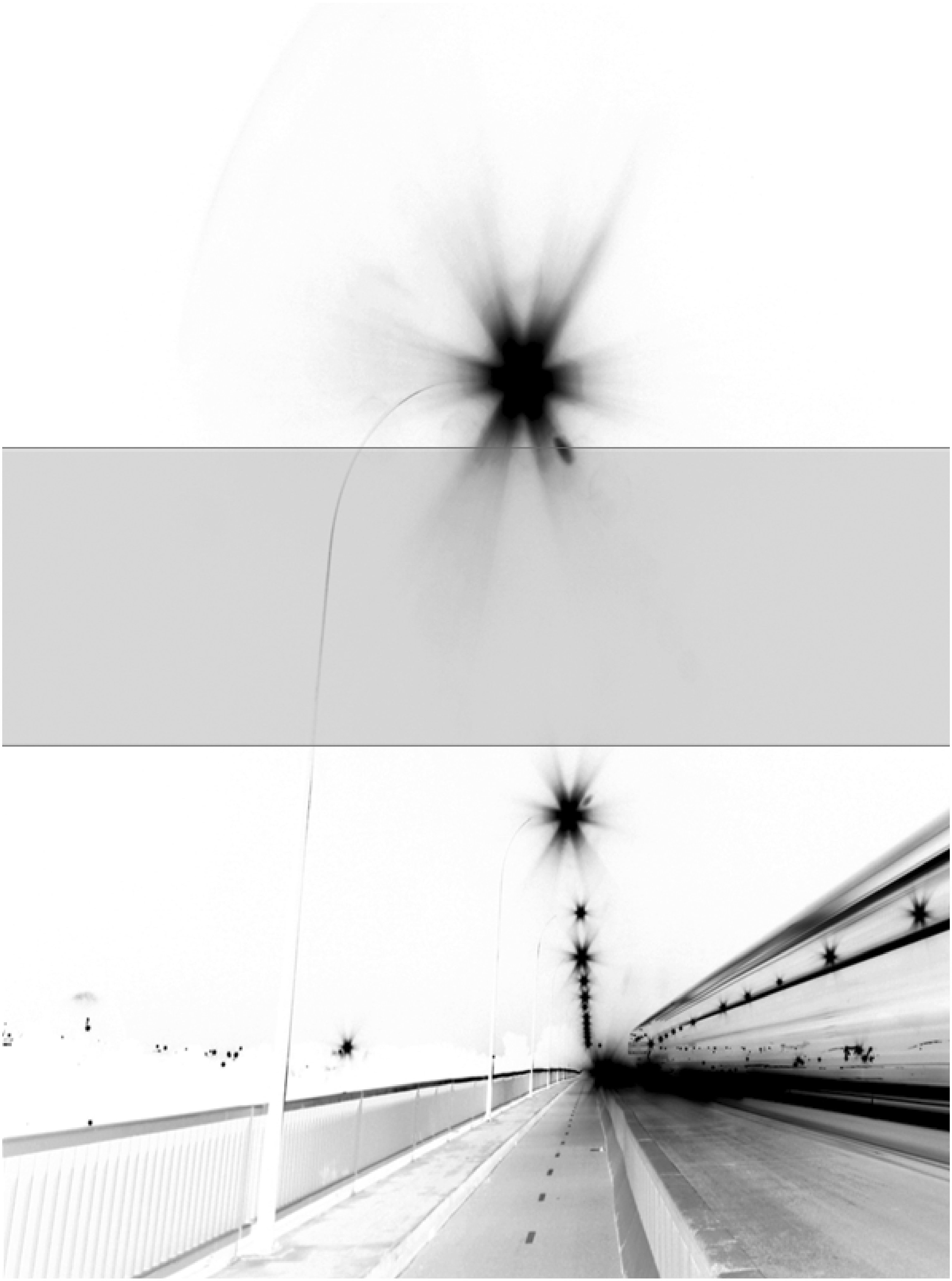
Managing Social Engineering Risk

- Making social engineering transparent -



Bernard Oosterloo



Managing Social Engineering Risk

- Making social engineering transparent -

Master thesis Industrial Engineering and Management

Author :

Bernard Oosterloo

Primary Supervisor :

Theo Thiadens

Secondary Supervisor :

Jeffrey Hicks

University of Twente
Enschede - The Netherlands

Primary Supervisor :

Peter Geurtsen

Supervisor :

Irene van Santen

Supervisor :

Peter Wemmenhove

Atos Consulting

‘Social engineering is lying, it just sounds better than saying you are a liar’

- Eric Cole, Insider Threat [COL05]

Preface

This thesis is the end result of the graduation project with the title 'Managing social engineering risk' and subtitle 'Making social engineering transparent'. This research project focuses on social engineering in organizations and addresses the following questions; what is social engineering and who is this social engineer, what are the threats to organizations, how can these threats be identified and which countermeasures can be taken to mitigate the risk of social engineering? The answers to these questions will lead to a social engineering risk management model to make the risks of social engineering more transparent and help organizations implement mitigating controls against social engineering.

This research was performed for Atos Consulting N.V., in order to model threats and countermeasures and develop a risk management model. It was performed by Bernard Oosterloo to generate a Master's thesis for the study Industrial Engineering and Management at the University of Twente.

I would like to thank all supervisors, colleagues and participants in the interviews for their support to this project and input for this thesis.

Enjoy reading!

Bernard Oosterloo

Utrecht, October 6th 2008

‘Please be good enough to put your conclusions and recommendations on one sheet of paper in the very beginning of your report, so I can even consider reading it’

- Winston Churchill

Management summary

A frequently overlooked factor in information security is the human, and more specifically the manipulation of a person to compromise information security. This thesis focuses on making the risks of this ‘social engineering’ transparent. And helping organizations manage these risks through a social engineering risk management model.

Research approach

The research consists of:

§ Elaborate theoretical research on social engineering and related subjects.

§ Qualitative empirical research verifying the theory, generating comments on a preliminary social engineering risk management model and requirements for the final model.

§ The proposal of a social engineering risk management model.

§ Conclusions and recommendations.

These will all be discussed in short next.

Theoretical research

This focuses on several subjects; the definition of social engineering, the social engineer, the attacks and possible mitigating controls.

Definition social engineering

For this thesis social engineering has been defined as follows:

> *The successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data.*

The social engineer

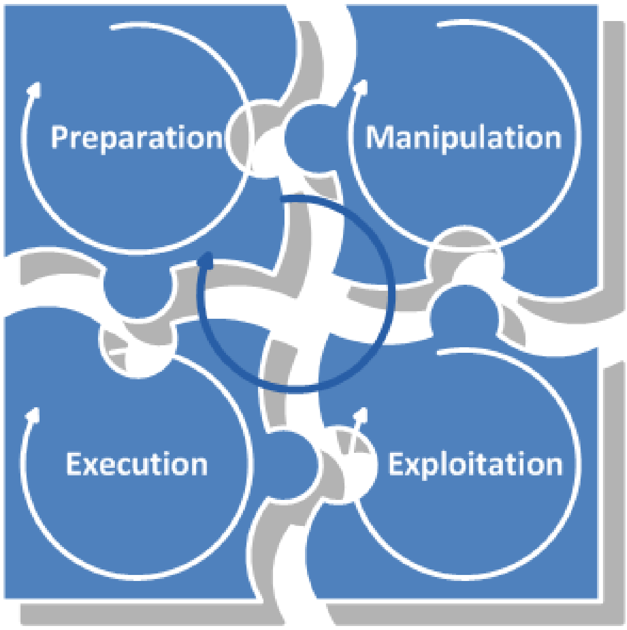
This thesis focuses on attackers that wish to harm the organization, the ones with *malicious intent*. As they are closely related to hackers, their overall motivation and personal motives are the same:

Social engineers	Social engineer’s motives
• Casual social engineer	• Financial gain
• Political social engineer	• Personal interest
• (Organized) criminal	• External pressure
• Internal agent	• Intellectual challenge
	• Damage containment

	• (Personal) grievance • Politics

Social engineering attacks

There are several models of the social engineering attack structure available, but none was complete. Therefore a new model was created:



Within the different phases in this attack structure several psychological principles and tactics are used to manipulate a person:

Psychological principles

- Strong affect
- Overloading
- Reciprocation
- Deceptive relationships
- Diffusion of responsibility
- Moral duty
- Authority
- Integrity
- Consistency

Social engineering tactics

1. Physical reconnaissance
2. People spotting
3. Dumpster diving
4. Forensic analysis
5. Phreaking
6. Phishing

11. Virtual impersonation
12. Reverse social engineering
13. Tailgating
14. Piggybacking
15. Office snooping/Desk sniffing
16. Item dropping

7. Mail-outs
8. Web search
9. Profiling
10. Physical impersonation
17. Data leakage
18. Direct approach
19. Identity theft
20. Malicious software

The following information has been identified as useful for the social engineer and should be classified as such:

Gathered information

a. Organizational structure
b. Employee names
c. Employee functions
d. New employees
e. Calendars
f. Internal phone numbers
g. E-mail addresses
h. Organizational policy and processes
i. Lingo
j. IT infrastructure
k. Organizational logos
l. User names
m. Passwords
n. Server names
o. Application names
p. Manuals
q. IP addresses

Mitigating controls

As most organizations already have (information) security controls in place a comparison of these with the list of possible security controls related to social engineering can be used to measure the current level of security. This list is given in chapter 5: 'Stop the social engineer' and is classified according to the function in security control *–general IT*, *prevention, reduction, detection, repression*, *correction* and *evaluation*- and to the level in the organization -*strategic, tactical* or *operational*.

Because this thesis focuses on the human factor in information security some important organizational and physical elements of the security architecture are highlighted:

Mitigating control focus

- Physical security
- Security organization
- Security policy and procedures
- Security awareness
- Security culture
- Monitoring and evaluation

Empirical research

The empirical research was performed to verify the theoretical research in practice and to validate stated lists, figures and models based on this theory. The theory verification was performed by challenging stated assumptions and hypothesis in the thesis as well as research and findings in studies used to base this theory on. Re-performance of some research in these studies was therefore necessary to verify questionable findings and findings from questionable research methods in these studies. For this research the qualitative information was gathered through *semi-structured in-depth* *interviews* with information and IT intensive and high risk organizations as well as the Computer Emergency Response Team of the Dutch government (GOVCERT), followed by a seminar discussion between several governmental organizations (national, municipal and penitentiary), an insurance company and organizers Atos Origin and Atos Consulting. The findings, related conclusions and recommendations helped get a feeling of how social engineering is perceived and mitigated in practice. The interviews where furthermore used to validate a preliminary social engineering risk management model and the seminar discussion was used to generate more specific needs and requirements of organizations on a final model. Both to structure the social engineering risk management model to be in line with the expectations and needs of real-life organizations.

Proposed social engineering risk management model

To minimize the potential of loss organizations need to manage social engineering risk which is defined as:

> *Social engineering risk management is a process, influenced by an organizations management and other personnel, applied across the organization, designed to identify social engineering risk and manage this risk to be below the predefined security level, to provide reasonable assurance regarding the achievement of an organizations objectives.*

The model to support organizations is based on elements of the Enterprise Risk Management

Integrated Framework (ERMF) of the Committee Of Sponsoring Organizations of the Treadway commission (COSO) as this is a commonly known framework for information risk management. The components of this framework have been used and filled further with steps more specifically related to social engineering.

Component	Steps
Internal environment	1. System and environment characterization
Objective setting	2. Objective setting
Event identification	3. Threat identification
Risk assessment	4. Vulnerability identification 5. Control analysis 6. Likelihood determination 7. Impact analysis 8. Risk determination
Risk response	9. Risk response 10. Control implementation 11. Residual risk evaluation
Control activities	12. Supporting policy and procedures implementation
Information and communication	13. Information and communication management

Monitoring	14.Ongoing monitoring 15.Periodic evaluation

Conclusions and recommendations

Following the steps of the model gives organizations the opportunity to measure and manage their social engineering risk level in a structured and transparent way. This leads to more security in achieving the organizations objectives.

However because of limited time and resources some things did not get into scope for this thesis:

Evolution

Because the field of social engineering is constantly evolving the proposed list of social engineering tactics needs to be kept up to date by regular updates a new tactics are only limited by the creativity of the social engineer.

Detailed risk management model

The proposed social engineering risk management model is still described on a high level. A more specific model should give the organization the means to support business continuity by better securing their assets through founded decision making, justifiable risk budgeting and clear documentation.

Specific controls

The COSO ERM framework and the social engineering risk management model are not specific enough. However the Control Objectives for Information and related Technology (COBIT) model provides a framework for risk management and control based on the COSO components. Many of its controls also apply to the mitigation of other information risks like social engineering. Also specific controls focusing on social engineering could be formulated to support a social engineering audit.

Research and test agreement

Clear boundaries should be set to how deep follow up research may go and how far testers can go when social engineering personnel. Therefore a challenge also lies in the structuring of an agreement process before research and for example a penetration test can be performed.

Overall

In general all controls and tools mentioned in this thesis should be elaborated and molded into practical tools, for the security officer, management and other personnel.

Table of contents

List of figures

List of tables

‘…people are the critical component of an effective information security program’

- Ed Zeidler, CISSP executive director (ISC)² [ISC06]

Introduction

Today there are many solutions to guard the hardware and software from intrusion of information (systems) by external parties and to some extent internal agents, but there is only limited research regarding the soft factors; the human factor in information security. [HIN05] [ISC06] Even if the very best technical solutions are in place to guard the information, still some personnel needs to have access and can thereby compromise this information security; intentional, unintentional or by manipulation. [MIT02] This research project focuses on '*social engineering*', the manipulated compromise. Mitigating the threats this manipulation poses will also reduce the intentional and unintentional compromising of systems and information. And therefore lower overall risk.

Relevance

The technical aspects of information security have been in the spotlight for several years, this has made much progress. In general, large improvements in security can no longer be attained by upgrades in hardware or software. [CAR06] It is therefore difficult for attackers to achieve their goal through technical attacks alone and their focus shifts (even more) to the organizations employees. [ALL02] As a result, organizations need to direct increased attention toward the heretofore under-treated human factor of information security to guard and stay in control of their (critical) information. For many organizations the weakest link in information security is now human. [ALL05] [HIN05] [ISC06] [JAN05] [KIE06] [MIT02] [SPE04] Organizations need to raise the security on this human factor to an even par with the technical security.

In response, information risk management is at the top of the training priorities for information technology security professionals. Organizations are looking to develop flexible frameworks that give insight in the risks involved and help them adapt to changing environmental factors. [CAR06]

There are a lot of articles, surveys and books which focus on the human factor or related subjects. But it is still a relatively unexplored field of scientific research. [CAR06] [KIE06] In most cases the articles and books do not have a scientific foundation and do not give a clear overview but merely discuss case descriptions or studies. However these studies show that the human factor can cause great damage to organizations, not only financial but also to the organization's image, which in turn influences the organizations goals and continuity in the long run. [COL05] [MIT02] [PRO06] [SPE04] [USS06]

Ironically, an organization's employees are not only important assets, but also pose a great threat because these employees know where to look and have the advantage of obtained trust and accessibility to systems and co-workers. [LAF04] [KRA05] Attackers can misuse these employees or could even be one of them. But acting on human weakness is only one way of attaining something you should not have access to. In some cases it is part of a technical *hack*, e.g. hacking into a server. So by preventing the information gathering through social engineering -also known as *people hacking*- the threat of technical hacking can be partially mitigated. [MIT02] [MIT06] This thesis will focus mainly on the threats from external parties but also, when applicable, relate these to threats from inside the organization. This will be discussed in the following chapters and accumulate in a high level social engineering risk management model. This can be used to gain transparency on the subject, implement mitigating controls and help organizations manage their social engineering risks.

But first the definition of ‘Social engineering’ used throughout the thesis will be given.

Social engineering defined

Social engineering has been defined in several ways -short or long- for example as:

§ *The unauthorized acquisition of sensitive information or inappropriate access privileges by a potential threat source, based upon the building of an inappropriate trust relationship with a legitimate user of an information technology system.*

Dudek, United States Department of the Interior [DUD06]

§ *Pretending to be something you are not, with the goal of tricking someone into giving you information they normally should not give and that you should not have access to. In short, social engineering is lying, it just sounds better than saying you are a liar.*

Cole: Insider Threat [COL05]

§ *Getting people to do things they wouldn’t ordinarily do for a stranger.*

Mitnick: The art of deception [MIT02]

§ *The act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information.*

Webopedia [WEB04]

§ *The practice of obtaining confidential information by manipulation of legitimate users.*

Wikipedia [WIK06]

But the following operational definition was chosen: [HAN03]

The successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data.

This definition was chosen because it covers all aspects of social engineering:

ü It covers not only successful acts but also attempts.

ü It may look like the word ‘influence’ was chosen poorly because it is very broad, but social engineers use a wide range of tactics, which are adequately covered by this word.

ü It covers access, use and disclosure as well as information, information systems, networks and data, which make it a complete definition.

Thesis outline

The thesis is divided into theoretical and empirical research. The theoretical research is described according to the research questions and is verified during the empirical research.

The thesis starts of with this introduction followed by a description of the project and the research problem. Next the theoretical research is discussed in chapters 3 through 5, which are based on a literature study on the research problem. In chapter 6 the empirical research is discussed to provide a solid base for the final design of a social engineering risk management model. Finally conclusions are drawn upon both the theoretical and empirical research, from which recommendations are rendered. More information and clarification of unfamiliar terms may be found in the more elaborate discussions in the appendices.

Summary

In summary, organizations still lack a consistent overall view of social engineering, which this thesis will try to generate. The thesis combines current research on social engineering with research in other fields and empirical research to make social engineering transparent for organizations and help them act on social engineering risk.

The next chapter will discuss the research problem and project approach.

‘We may not realize we have a problem, but that does not stop us from having one.’

- Michael J. Hicks, Problem solving in business and management [HIC04]

Project description

The short analysis in the introduction already uncovered that the knowledge on social engineering of organizations and their information technology professionals is still insufficient to cope with the risks related to social engineering. In this chapter the research project will be further discussed with the research problem, project scope and research approach.

Problem

During the research project models, methods and finally a social engineering risk management model are generated on the basis of both existing and new (empirical) research. The goal of this project was to find out how to strengthen the weak link in information security, the human factor, by looking at:

§ How social engineering occurs in organizations.

§ The measures that can be used to stop social engineering from causing harm.

§ How an organization can measure the risks and their protection from social engineering threats and if necessary apply appropriate countermeasures to mitigate these risks and stay in control of their information, thus ensuring business continuity.

Problem definition

To ensure business continuity and give organizations a clear view on social engineering, the problem is defined as follows:

> *There are no tools available to measure the risks social engineering imposes on organizations and which countermeasures they can take to mitigate these risks.*

This is a conjunction of more specific problems:

§ Organizations are unaware or are not interested in the risks social engineering imposes on them.

§ Organizations have problems to recognize and detect social engineering.

§ Mitigating controls and countermeasures are unknown or organizations are not familiar with them.

§ Measurement tools regarding social engineering risk are not in place or are unknown.

Main research questions

The problem definition defines a design problem and can therefore be divided into three successive main research questions[1]: [SWA01]

1. *Which risks do organizations run as to social engineering?*
2. *Which countermeasures can be taken by an organization to protect themselves against the threats of social engineering?*
3. *How can organizations measure the social engineering threat and mitigate the risks it poses?*

These main research questions are answered by the research and set the basic scope of the project.

Deliverables

The deliverables from the research can be summarized according to the main research questions:

1. Description of social engineering and its risks

The answer to the descriptive research question will present a definition of social engineering and the social engineer in the context of the research project, a model of an attack, a summary of the applied tactics and targeted information and an assessment of the risks these threats pose on the organization.

2. Measures to stop the social engineer

The answers to the remedy research question will present controls and measures which can be implemented against social engineering attacks.

3. Design of risk measurement and management tool

The answer to the design research question will present a basic design of a social engineering risk management model. The risk management model can be specified to fit the organization and can be used to measure the risks of social engineering posed on an organization and gives an advice on mitigating actions the organization can take to lower these risks.

Project scope

All aspects of influence to the social engineer and the organization are summarized in the following ontology[2] -based on Schumacher [SCH06]- with the attacker on the left and the stakeholders on the right:

[1] The design problem and related questions and deliverables are discussed more elaborate in Appendix A: Notes chapter 2.

[2] An ontology models part of the world and is used to 'establish a common understanding of relevant concepts, the relations between them and inference rules'. [SCH06]

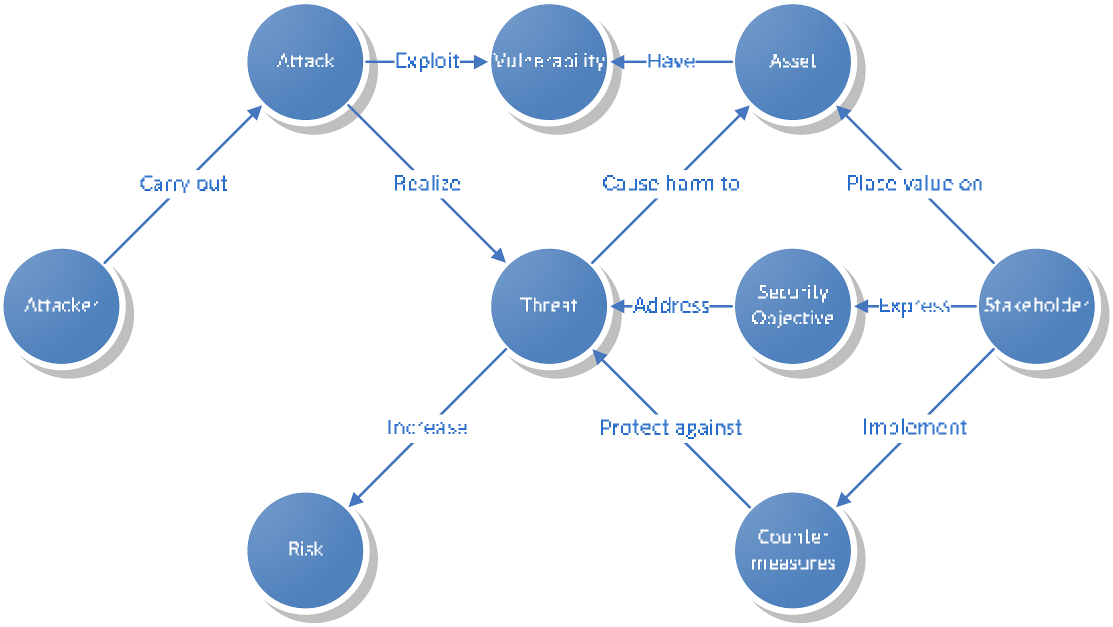


Figure 1: Ontological chart of social engineering

From left to right and top to bottom:

- An *attacker* is the entity which carries out attacks; in this case the social engineer –external or internal- as discussed in chapter 3. [SCH06]
- An *attack* is a deliberate action that violates the security[3] of an asset; in this case the structure of tactics as discussed in chapter 4. [SCH06]
- *Vulnerability* is a flaw or weakness that can be exploited to breach the security of an asset; in this case the focus is on the human as weakness and gateway to specific information which creates vulnerabilities, discussed in part in chapter 4 and chapter 7. [VER01]
- A *threat* is an action or event that might violate the security of an asset; in this case the threat of loosing *confidentiality*, *integrity* or *availability* of information, information systems, a network or data by an act of an attacker. [MAI03] [SWA01] The tactics underlying the threats are discussed in chapter 4 and elaborated on in chapter 7.

[3] Security is a condition of safety from threats. [SCH06]

- *Risk* is the potential of loss that requires protection; in this case the loss of control over the information, information systems, networks or data. [MAI03] The management of this risk is discussed in chapter 7.

- An *asset* is anything –tangible or intangible- of value to the stakeholders; in this case information, information systems, a network or data and the control thereof as stated in the definition of social engineering in chapter 1.

- A *stakeholder* is anyone who has an influence on the organization –e.g. management, employees and legislators- or is influenced by the organizations operations –e.g. shareholders, customers and suppliers-. The stakeholders this thesis focuses on are the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) who need to commit to the mitigation of social engineering risk and support this process to make it successful.

- A *security objective* is the level of security an organization wishes to achieve linked to a specific threat; every organization needs to state these objectives for themselves keeping the budget and other resources in mind. This is discussed shortly in chapter 7.

- A *countermeasure* is an action taken in order to protect an asset against threats and attacks, in this case all applied controls and measures to counter the social engineer in succeeding in his or her endeavor. [VER01] These are discussed in chapter 5.

This research starts with the attacker, attack and measures, to form a basis for the social engineering risk management model which links to the entire chart. Technical aspects are not researched unless in context with one of the social aspects. More specific restrictions on the scope will be given in the thesis as they come along.

Research approach

In search of an appropriate method to tackle this kind of problem several different approaches are suggested in literature. Because of the project's time limit a clear approach was necessary with clear control means. Insights from several approaches are combined to meet the needs of the project.

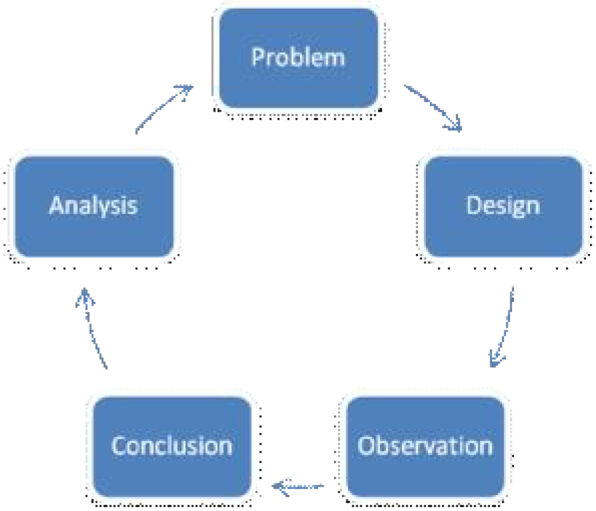


Figure 2: Empirical cycle for complex problems

For the basis of the project plan and the basic framework of the research project the book “Van probleem naar onderzoek” of Geurts was chosen. [GEU99] This book focuses on building a research project around a problem and uses the *empirical cycle* and theory of Swanborn. [SWA90] It is not followed strictly but all elements of the cycle were covered in the project plan or in this thesis.

In addition to Geurts, insights are taken from the structured project management method Project IN Controlled Environments (PRINCE2). The method divides the project into manageable stages which makes it easier to control and monitor the progress. [KEY06] For this small project the complete PRINCE2 method is not suitable, but the elements *project assurance* and *control of change* have been added to the approach already stated by Geurts and Swanborn. And finally a project risk assessment has been made using a project risk model.

This theoretical background is discussed in greater detail in Appendix A: ‘Notes Project description’.

The following chapter will start off with a discussion on the social engineer in relation to the well known (technical) hacker.

‘If you know your enemy and know yourself, you need not fear the result of a hundred battles.’

- Sun Tzu, The art of war [SUN98]

Hackers and social engineers

Hacking and social engineering are closely related. Social engineering tactics are applied to gather information in preparation of a hacking scheme and the motives and goals of both types of attacker are related. They are even so similar that social engineers are also known as ‘*people hackers*’. It is therefore important to know who these (people) hackers are. In this chapter a description of hacking and the hacker will be given along with the motives a social engineer may have.

Hackers, crackers and phreakers

There are hackers with good intentions that for example search for vulnerabilities so organizations can patch them. But there are also hackers with bad intentions that use these vulnerabilities to cause harm or to achieve personal gain. As a consequence the term hacking is not always used correctly in the media.

There are three types that all get the predicate ‘hacker’ in the media; hackers, crackers and phreakers. [RAY03]

- The jargon dictionary defines a *hacker* as: ‘A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary’ and ‘one who enjoys the intellectual challenge of creatively overcoming or circumventing limitations’. [RAY03] A hacker is therefore someone who seeks challenges and overcomes boundaries using his or her skills. Hackers follow an ethical code and do not act illegally, which differentiates them from the crackers. [BEA04]

- A *cracker* in contrast is someone who breaks into the system of a person or organization with the goal of theft or vandalism and therefore does not act ethically. The crackers form small groups within the hacking community and are seen as ‘a lower form of life’ by other hackers. Another name for these crackers is ‘dark-side hackers’. [RAY03]

- And finally *phreakers* use information and social engineering skills to break into telephone systems and use these for various purposes, for example making long distance phone calls at another’s expense, stealing phone card numbers or pretending to call from a secure location. [RAY03]

Whenever the term hacker is used in this thesis the hackers with malicious intent -the crackers- are meant.

People hackers -in contrast to technical hackers- focus on the weaknesses in the human, instead of the technology they use. The people hackers referred to in this thesis all have malicious intent and could therefore be classified as ‘people crackers’ according to previous classification. The definition of a social engineer used in this thesis is therefore as follows:

> *A social engineer is a hacker of people, with malicious intent.*

This definition excludes the social engineering acts without malicious intent that happen consciously and unconsciously in day to day life, but includes the phreakers if they intend to use their access to the telephone system for malicious purposes and obtain this access by influencing people.

Attackers motives

Knowing why *attackers* –hackers or social engineers- might attack is crucial for estimating the likelihood of a social engineering attack on a specific organization and to implement appropriate measures and controls to counter this attack. [LAF04] [ROG02] [ZAG02] The motivation of different subcultures within the hacking community will now be discussed followed by the motives of the social engineers.

Hacking subcultures motivation

Zager identifies four subcultures within the hacker community each with different motivation; casual hackers, political hackers, organized crime and internal agents. [ZAG02]

§ *Casual hackers* form the largest group. They are motivated by curiosity or the challenge of getting into the system. Their goals are varied from just mischief to actual theft and are very important to gaining acceptance in the hacking community and notoriety by their achievements. [ZAG02] They often use tools created by more skilled people as they are not as skilled in general and can target any organization. [LAF04]

§ *Political hackers* hack for a cause and are also called cyber activists. They use their skills to give publication to their cause or attack organizations that represent interests against their cause. But many hackers who profile themselves as political hackers 'use their infantile perspective on the world's politics as justification, while their real motivation is demonstrating that they can take over a website', according to Richard Stiennon, Gartner research director for network security. [LAF04] There are therefore only few genuine political hackers. Cyber terrorists fall in this group. They can cause massive damage for their political beliefs and focus on critical infrastructure. [ZAG02]

Private as well as governmental organizations can be targets of a political hack. Every highly visible organization is therefore at risk.

§ *Organized crime* consists of professional criminals. These organized crime rings are growing in number and activity in the former Soviet Union and several African countries and pose a serious threat to organizations with valuable information, for example, credit card numbers or trade secrets. [ZAG02]

§ *Inside agents* include organization employees as well as trusted third parties like external consultants and suppliers. They can cause great damage because of their place within the organizational boundary. Most inside attacks are motivated by curiosity, which can lead to theft, but vandalism from former employees also occurs. [ZAG02]

Lafrance adds another group, *squatters*, which do not target specific organizations but use the accessed systems for storage, to spread viruses and worms, or as zombie systems to be used in so called 'Distributed Denial of Services' (DDoS) attacks. [LAF04]

In these communities another categorization can be made in *external* -casual hackers, political hackers, organized crime, squatters– and *internal* -internal agents. [LAF04] This classification on the connection with the target organization is important, because the internal agent can cause greater damage with less effort. [SPE04] For now the focus is foremost on the external attackers.

Social engineer's motives

There are also hackers that do not act as a member of a subculture. The Australian government performed research on the (personal) motives of a hacker. [AIC05] The motives of the attacker – hacker or social engineer– can be classified according to a variation on the results of this research. For each category a general description of the motive is given, a classification in malicious or good/benign intentions and what role social engineering can play in an attack with this motive.

1. Financial gain

These attackers are after financial gain and focus on money, valuable data, services, capacity or intellectual property, extortion, fraud and marketing schemes. This kind of attack requires a great deal of planning and preparation to be a success and to remove all traces that could lead back to the attacker. [AIC05]

The intentions of the attacker are malicious, the target will always be harmed and suffer financial or other damage.

Social engineering is a technique used extensively to gather information to prepare and execute the attack.

2. Personal interest

This includes entertainment and curiosity. Attackers focus on the access, change or removal of information. Removing traces is not a high priority and it requires little preparation and can be performed on the spur of the moment. [AIC05]

The intentions of the attacker are not malicious but an attack can still cause great damage.

Social engineering can be used to gather information, prepare for another form of attack or be used to get to the final access, change or removal of information.

3. External pressure

This includes the pressure to demonstrate skills to stay or be accepted in a social group or upholding a certain status -and with that power- within this group. It also includes the pressure of relatives, friends and organized crime to influence an individual or organization. This can take on many forms, for example blackmail or just returning a favor.

The motive is therefore the relief of –part of– the pressure by acquiring a certain status within the social group or helping relatives, friends or organized crime. An individual can be pressured for example because of his or her place in the target organization; to misuse their social status or job function. [AIC05]

The intentions of the attacker are derived from the intentions of the social group or person that applies the pressure. With organized crime it is clear that the intentions are malicious and will in the end harm an individual or organization.

Social engineering can be used to gather information, prepare another form of attack or be used to achieve the final goal of the attack.

4. Intellectual challenge

Attackers focused on an intellectual challenge are not necessarily after recognition. The attacker wants to prove something is possible and targets secure or high profile organizations and people.

The intentions of the attacker are not by definition malicious but the technical tools used –*worms, viruses, Trojan horses*– can cause great damage or create vulnerabilities that can be abused by other attackers. [AIC05]

The way social engineering can be used in an attack is subject to the goal of the attack; if the goal is to acquire specific information, social engineering can play a great part in the attack. But the main challenges taken up by attackers are still technical; in most cases therefore social engineering will be used to gather information and prepare for the final attack.

5. Damage containment

An attack can also focus on the minimization of damage from a previous attack –that may have been malicious– or try and help individuals and organizations to patch vulnerabilities in their systems and network. [AIC05]

Although the intentions of these attacks are not malicious the outcome can still cause damage when the attack is performed with unfamiliar tools.

By means of social engineering the attacker can for example help individuals and organizations to change their settings or delete malicious software. And it can again be used to gather information and prepare another form of attack.

6. (Personal) grievance

In this case grievances are very general and include claim of right, revenge and vigilantes. The attack is based on a feeling of injustice. Attacks can target an individual or organization to retrieve something that the attacker believes is his or hers, or just to damage the individual or organization that has caused this injustice. [AIC05]

The intentions of the attacker are malicious because something is taken from the target or the attack causes harm, even though the attacker is alone in his or her perception of having suffered.

Social engineering can be used to gather information, prepare another form of attack or be used to achieve the final goal of the attack.

7. Politics

The causes that lay underneath these political attacks can be for example religious, political, environmental and can lead in extreme form to terrorism. The focus of the attack is in most cases an individual or organization that represents interests against their cause or is highly visible. Attacks on these people or organizations can generate great publicity to the cause. Cyber terrorists can cause massive damage for their beliefs and focus more on critical infrastructure. [AIC05]

The intentions are malicious as activists will do anything to get publicity for their cause.

Social engineering can be used to gather information, prepare another form of attack or be used to achieve the final goal of the attack.

Conclusion

From this classification it is clear that social engineering can play an important or just basic role in an attack, but in both cases can lead to great damage for the targeted organization or individual. Although the intentions of some attackers are not malicious they can still cause great unintentional damage. It is therefore important to stop all these attacks and leave the patching and investigating to the experts.

Summary

In this chapter the hacker, the hacker community and the motives of a hacker and social engineer are discussed.

§ The (people) hackers this thesis focuses on are the ones with malicious intent –to cause harm by vandalism or theft- the so called crackers.

§ For organizations it is very important to know which motives an attacker might have and with this to be able to make an assessment of the likelihood they will be attacked by a hacker or social engineer. With this knowledge specific countermeasures can be implemented. To understand the hackers the motivations of different subcultures are discussed, these can be divided into external –*casual hacker, political hacker* and *organized crime*- and internal –*internal agents*. Next to the group motivation a list of social engineer's personal motives are discussed, these can be; *financial gain, personal interest, external pressure, intellectual challenge, damage containment, (personal) grievance, politics*.

These classifications can be used for measurement and mitigation of an organization's risk in the social engineering risk management model as discussed in chapter 7.

The different social engineering attacks will be discussed in the next chapter.

‘The classification of the constituents of a chaos, nothing less here is essayed.’

- Herman Melville, Moby-Dick [MEL06]

Social engineering attacks

Social engineering is still a growing threat but social engineering and the threats associated with it are not always recognized by organizations. In this chapter an analysis of social engineering attacks will be discussed with the tactics used by the social engineer, followed by several classifications of these tactics.

Attack strategies

To create a step-by-step strategy which can encompass all attacks, two existing models are discussed and elements of both models are used to create a model which encompasses social engineering attacks.

Attack cycle

Allan proposes a social engineering attack as a cycle. It consists of four phases: Information gathering, relationship development, exploitation and execution. [ALL05] [ALL06]

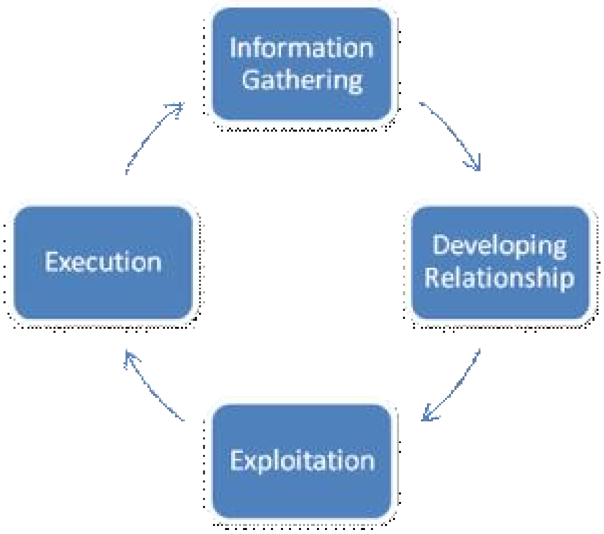


Figure 3: Attack cycle by Allen

1. *Information gathering* -research- can be performed with various techniques and covers information on the organization –e.g. phone lists, organizational charts, lingo[4]– or on intended targets of an attack –personal information. [MIT02] This information is used in the next phases to gain trust. [ALL05] [ALL06] [GRA01]

2. To *develop a relationship* trust is necessary. [MIT02] The human is trustworthy by nature and a relationship can be developed easily with the proper knowledge obtained in the previous phase.

[4] Lingo is language used within a specific group or organization, also known as jargon.

[ALL05] [ALL06] [DOL04] [GRA01] The relationship can be used to execute the attack or give the attacker more information to fill in the puzzle.

3. During the *exploitation* the target can be influenced by the trusted attacker to 'reveal information or perform an action that would normally not occur'. [ALL05] [ALL06] [MIT02]
4. The *execution* phase can be interpreted as the execution of the last step in an attack if the obtained access or information is not the final goal and the attacker still needs to execute the final act using the obtained trust and information, for example entering an information system to steal, change or delete files. [ALL05] [ALL06] [MIT02]

Attack series

Janssen gives another interpretation of the four phases based on the goals an attacker wishes to accomplish during a phase: *Global information gathering, specific information gathering, gaining access to information systems, realizing final goal*. [JAN05] The difference is linked to the placement of the phase beginnings and ends, which are at different moments than in Allen's attack cycle. In this interpretation the gathering of specific information is more emphasized then the way in which this information is obtained.

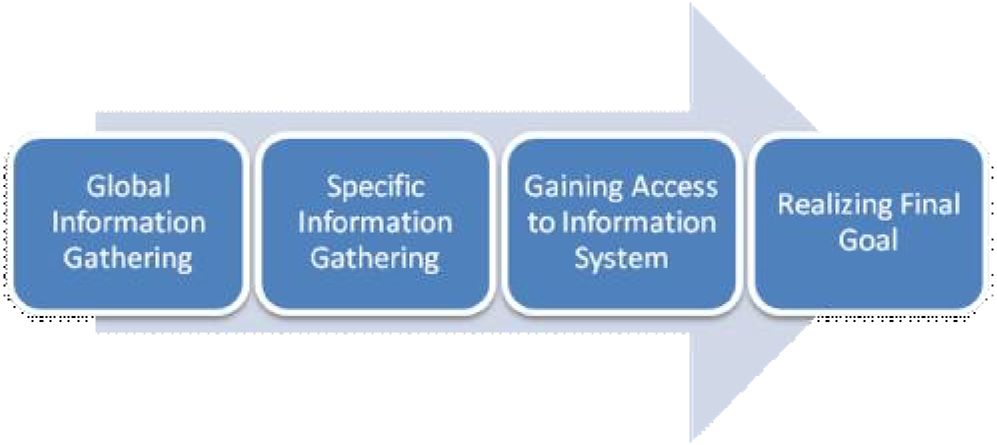

Global Information Gathering
Specific Information Gathering
Gaining Access to Information System
Realizing Final Goal

Figure 4: Attack series by Janssen

Best of both worlds

Comparing the two models, both attack models have a specific focus; the first focuses on developing a relationship as means of getting someone to act, which is only one way of manipulation. The second focuses on the access of information systems which is specific and narrow. It is furthermore modeled as a series instead of a cyclical and iterative process.

A tailored version of the cycle by Allan will be used within this research project. The tailored version consists of the phases: Preparation, manipulation, exploitation and execution.

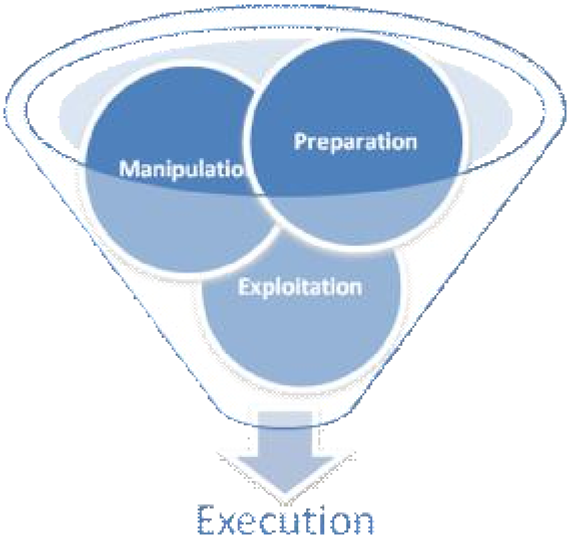


Figure 5: Basic attack elements

Phase 1: Preparation

The first phase consists of all *preparation* before engaging a target –also known as footprinting- which includes information gathering but also the gathering of other (physical) attributes needed in the next phases, like recreating letterheads and learning the lingo. [DOL04] These attributes and knowledge can be used for the manipulation in the next phase.

Social engineering tactics applied[5]:

1. Physical reconnaissance
2. People spotting
3. Dumpster diving
4. Forensic analysis
5. Phreaking
6. Phishing
7. Mail-outs
8. Web search
9. Profiling

One thing all these tactics have in common is that the personnel distributing the information –in any way- do not know the value of the information to the social engineer or hacker.

[5] The social engineering tactics are described in Appendix B: 'Notes Social engineering attacks'.

Important information gathered in this phase:

a. Organizational structure
b. Employee names
c. Employee functions
d. New employees
e. Calendars
f. Internal phone numbers
g. E-mail addresses
h. Organizational policy and processes
i. Lingo
j. IT infrastructure
k. Organizational logos
l. User names
m. Passwords

Phase 2: Manipulation

It is part of human nature to trust people easily and to want to help people. [JON03] [GRG02] A social engineer will exploit these tendencies to manipulate targets in doing what the social engineer wishes. [ALL05] [ALL06] [GRA01] [JON03] [MIT02] The manipulation phase consists of all ways of influencing the target to create authenticity and obtain trust. This *manipulation* can be performed physically –physical interaction between the social engineer and target- or virtually –by means of a medium e.g. phone, fax, e-mail. [ALL02] It can be used to gather more information or lead to the exploit of a target and execution of the attack. [ALL06]

Basic psychological principles underlying manipulation[6]: [GRG02] [CIA00]

Psychological principles	
§ Strong affect	§ Moral duty
§ Overloading	§ Authority
§ Reciprocation	§ Integrity
§ Deceptive relationships	§ Consistency
§ Diffusion of responsibility	

Table 1: Psychology principles

[6] The psychological principles are described in Appendix B: Notes Social engineering attacks

In summary all these psychological principles focus on the creation of a feeling of trust or a situation in which the target will not be likely to challenge the request of the social engineer, creating vulnerabilities in the security.

Social engineering tactics applied:

10. Physical impersonation
11. Virtual impersonation
12. Reverse social engineering

During the usage of these tactics the social engineer can increase the chance of success by avoiding conflict using a less aggressive approach, appealing to other senses like sound and sight to strengthen the relationship and most importantly; the social engineer needs to be able to think fast and be willing to compromise. [ALL06]

Important information gathered in this phase:

No specific information is gathered in this phase. The manipulation sets the target up for exploitation in the next phase. The manipulation and exploitation therefore have a strong link.

Phase 3: Exploitation

The *exploitation* is the use of the influence on the target to ‘reveal information or act in a manner that results in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data’, in accordance with the definition of social engineering.

Social engineering tactics applied[7]:

10. Physical impersonation
11. Virtual impersonation
12. Reverse social engineering
13. Tailgating
14. Piggybacking
15. Office snooping/Desk sniffing
16. Item dropping
17. Data leakage
18. Direct approach

The trust and influence over the target obtained through the manipulation in the previous phase is used to enter the target location and/or in applying other tactics.

[7] The tactics and information in gray indicate they have been addressed in an earlier phase.

Important information gathered in this phase:

a. Organizational structure

b. Employee names

c. Employee functions

d. New employees

e. Calendars

f. Internal phone numbers

g. E-mail addresses

h. Organizational policy and processes

i. Lingo

j. IT infrastructure

k. Organizational logos

l. User names

m. Passwords

n. Server names

o. Application names

p. Manuals

q. IP addresses

In this phase new information can be gathered or more specific information not obtained in the first phase.

Phase 4: Execution

The *execution* phase follows the interpretation of Allen and consists of actions that are not specifically related to social engineering or are the beginning of a new cycle. [ALL06] Attacks and countermeasures in this phase mostly have a technical nature and are more in the fields of hacking or plain theft then social engineering. [DOL04] But the following actions attract special attention because of the importance of social engineering in their execution.

Social engineering tactics applied:

7. Mail-outs

19. Identity theft

20. Malicious software

This malicious software can have the form of a virus, Trojan horse or worm.

Information gathered in this phase:

Information gathered in this phase is dependant of the goal of the social engineer but can consist of all information available on the organizations infrastructure –all organizations information systems and physical locations– for example more specific plans of a new invention; industrial espionage. [JAN05]

Overall attack

An overall *attack* can consist of multiple cycles and can be seen as the overall puzzle consisting of several pieces, each of which is another puzzle in itself, a single cycle according to the model of

Allen. [DOL04] During an attack specific phases or tactics can be performed multiple times before going to the next phase. Performing an attack or even going through a single cycle is therefore an iterative process that will finally yield the anticipated outcome for that specific piece of the puzzle. The tactics used during an attack or cycle depend on the skills and motives of the social engineer. [LAF04]

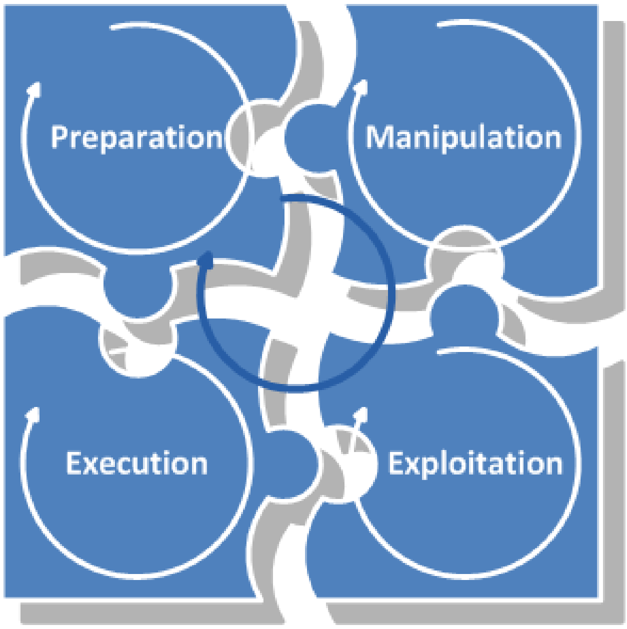


Figure 6: Overall attack structure

The time spent on an attack is dependant on the level of preparation, encountered resistance and magnitude of the attack. The time spent on the preparation comprises –when performed correctly- the longest phase in the attack (cycle) and shortens the time spent on the other phases. [ALL06]

In summary the social engineering tactics and gathered information:

Social engineering tactics

1. Physical reconnaissance
2. People spotting
3. Dumpster diving
4. Forensic analysis
5. Phreaking
6. Phishing
7. Mail-outs
8. Web search
9. Profiling
10. Physical impersonation
11. Virtual impersonation
12. Reverse social engineering
13. Tailgating
14. Piggybacking
15. Office snooping/Desk sniffing
16. Item dropping
17. Data leakage
18. Direct approach
19. Identity theft
20. Malicious software

Table 2: Social engineering tactics applied

Gathered information
a. Organizational structure
b. Employee names
c. Employee functions
d. New employees
e. Calendars
f. Internal phone numbers
g. E-mail addresses
h. Organizational policy and processes
i. Lingo
j. IT infrastructure
k. Organizational logos
l. User names
m. Passwords
n. Server names
o. Application names
p. Manuals
q. IP addresses

Table 3: Information gathered and used in social engineering attacks

These lists are only the tactics and important information known at this time. Because the field of social engineering is still evolving new tactics will be created and new information will be targeted. This will be further discussed in the recommendations.

Summary

In this chapter a model of the structure of a social engineering attack is given, the different tactics used by social engineers are summarized and the relevance to the research is discussed.

§ The *attack* structures by Allen and Janssen are fused into a new structure consisting of the phases; *preparation, manipulation, exploitation and execution*.

§ In each phase specific tactics are used to obtain specific assets -information or attributes- or manipulate people into 'revealing information or acting in a manner that results in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data' to get to the final goal of the attack.

The information gathered from the different tactics during the attack -*secondary targets*- is necessary to reach the final goal -*primary target*- of the social engineer, whatever this may be. [DOL04] By stopping the social engineer from obtaining this information the final goal cannot be reached, which creates a basic security for the targeted asset. [LAF04]

The next chapter discusses the countermeasures which can make it possible to mitigate the risks of social engineering.

‘To resolve a problem is to select a course of action that yields an outcome that is good enough, that satisfies.

To solve a problem is to select a course of action that is believed to yield the best possible outcome that optimizes.

To dissolve a problem is to change the nature of, and/or the environment, of the entity in which it is embedded so as to remove the problem.’

- Russell Ackoff, The art and science of mess management [ACK81]

Stop the social engineer

To stop the social engineer from succeeding or even damaging the organization's assets organizations need to apply measures to counter the social engineering attacks and tactics. They can change the environment of the asset, they can choose to act on occurring attacks or they can mitigate the social engineering risk by the structured implementation of countermeasures. This thesis focuses on transparency of social engineering and therefore on the *structured* implementation of countermeasures. In this chapter the information security controls –which encapsulate several measures to mitigate the social engineering risk- will be classified and listed. After which the key elements pertaining to the human factor are discussed in more detail.

Information security controls

Organizations need to implement controls to secure their information. In literature several classifications are proposed to make the choice and implementation of information security controls more transparent. Bautz cube defines the most dimensions and is regularly cited. It classifies organizational security in three dimensions; [THI02]

§ *Reason of protection*; to protect confidentiality, integrity or availability.

§ *Kind of measure*; physical, logical or organizational.

§ *Moment of action*; corrective, repressive, preventive and detective.

Most other models do not classify the reason of protection. Because social engineering threatens the confidentiality, integrity and availability the implemented controls need to protect against all of these. Therefore this dimension will not be elaborated on. [STO02] [SWA01]

For the classification of the information security controls a variation on Bautz cube is created. This classification is based in part on a classification by the United States National Institute of Standards and Technology (NIST) and complemented with input from the IT Infrastructure Library (ITIL). These both classify the controls on two dimensions. The classification proposed here also consists of two axes, the first according to the *function of control*, the second according to the *level in the organization*.

Function of control

The function of a control is related to its place and effect in the security management process. [CAZ99] The ITIL classification for security management is used to complement and add an extra level to the process defined by the NIST as this only discusses a limited number of functions and is not as transparent:

§ *Preventive controls* need to be implemented to prevent *threats* -possible social engineering attacks- from occurring and becoming an *incident* causing damage. [CAZ99] [MAI03] [STO02] [SWA01]

§ *Reductive controls* can be implemented to minimize possible damage from successful or attempted attacks but do not prevent the incident from occurring. [CAZ99]

- *Detective controls* need to be implemented to detect social engineering attacks as they occur, to be able to act on them and to develop and implement new preventive controls. [CAZ99] [STO02]

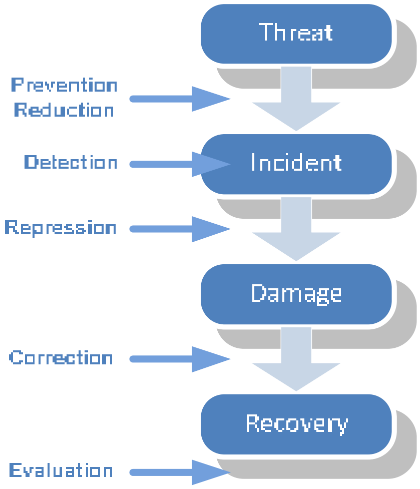


Figure 7: Controls in security organization

- *Repressive controls* can be implemented to stop the incident from continuing to cause damage or reoccurring. [CAZ99]

- *Corrective controls* need to be implemented to recover from damage caused by the social engineering attacks and restore availability after an attack has occurred. [CAZ99] [STO02]

- *Evaluation* should take place when a serious security incident has taken place to determine the cause, consequences and possible solutions to prevent the incident in the future. [CAZ99]

To support the specific controls against social engineering some *general security controls* need to be implemented. These form a base for the more specific controls and will probably -in part- be implemented already to protect other assets from other forms of attack.

Level in the organization

The second classification states that organizations need to implement a mix of technical and non-technical -management and logical- security controls. [CAZ99] [STO02] [SWA01] These relate to the level in the organization the controls pertain to:

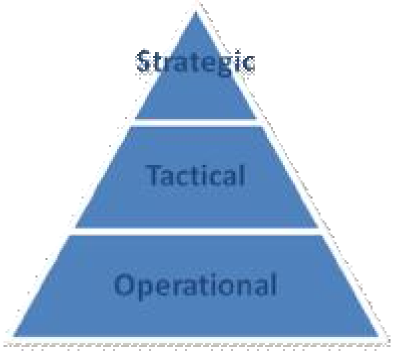


Figure 8: ITIL layers in security management

- *Strategic security controls* focus on the information security policy, guidelines and standards the *management* of an organization can lie down to build procedures upon to guarantee business continuity. [STO02] The management is furthermore responsible for the correct implementation of the policy and guidelines in procedures and operational controls. [DOL04]

- *Tactical security controls* are the implementation of the security policy in procedures and work instructions for personnel. [STA02] [STO02]

- *Operational security controls* are the operational implementation of the procedures and actions according to predefined work instructions. They can also consist of *technical* 'safeguards' in hardware, software or firmware to support the operational security and physical access control. [STA02] [STO02]

The tactical and operational security controls can be used to identify and communicate vulnerabilities in the organization to the management and are a translation of the vulnerabilities and related strategic controls identified by management.

Security controls classification

The information security controls proposed by the NIST form a basis for the controls organizations can implement to counter social engineering risk. [STO02] Possible information security controls related to social engineering are listed in the following table according to the previous classifications.

Classification		Control
General	Strategic	Security culture Security policy Ongoing risk management
	Tactical	User awareness procedures Data classification procedure
	Operational	Security awareness and technical training Data classification Segregation of duties Basic identification measures System protection features Key management
Preventive and reductive	Strategic	Risk assessment Security documentation and planning Security responsibility assignment Personnel security
	Tactical	Authentication procedure Authorization procedure Data media usage Non-repudiation Protected communication measures Transaction privacy measures
	Operational	Access control enforcement Data labeling and distribution Malicious software prevention

		Offsite storage Facilities safeguarding Physical systems protection
Detective and repressive	Strategic	Audit policy
	Tactical	Incident response procedure Periodic control review Periodic audit
	Operational	Internal & external audits Intrusion detection Malicious software detection Incident response Intrusion containment
Correction	Strategic	Recovery policy
	Tactical	Backup procedures Recovery procedures Disaster recovery plan
	Operational	Security state restoration Malicious software removal
Evaluation	Strategic	Ongoing risk management
	Tactical	Logging procedures Evaluation procedures Non-repudiation
	Operational	Logging activities Security documentation

Table 4: Information security controls related to social engineering

More elaborate descriptions of and discussions on these controls can be found in the referred literature. The focus now is on the more specific controls against social engineering attacks.

The human factor

Several of the previous controls should already be in place to stop hackers or intruders. Most *software*[8] and *hardware* therefore only need an upgrade to also filter for social engineering attacks. *Physical* entry controls should for example already be at a level fitting the asset needing protection. But because no technical or physical control can stop a social engineering attack by itself it is important to focus on the *organizational* measures and add the knowledge about social engineering and the applied tactics to the consciousness of the personnel to stop the social engineer from by-passing these existing security measures and rendering them useless. [CAR06] [WIN95] This weak human link in the security chain needs to be reinforced by clear security objectives in the form of controls, policy, standards and procedures pertaining more specifically to social engineering. And implementing organizational countermeasures in the form of an awareness program related to

[8] Starreveld states a classification of the measures in physical, organizational, hardware and software measures. [STA02]

social engineering to stop the social engineer from damaging organizational assets and embed social engineering awareness in the organizational culture, which is a countermeasure in itself. [MIT02] [SCH06] The Information Systems Audit and Control Association (ISACA) identifies several key elements of information security management. The organizational security measures attained from the research will be highlighted below according to these elements, after the physical security is shortly addressed. [ISA06]

Physical security

Physical security needs to be in order to stop physical social engineering attacks. *Access controls* need to be in place to stop unauthorized access, but must not interrupt the access of authorized persons. [RED05] A balance between these two should be found. A first step in access control is authentication through *identification*. This could be established by a password, a token –e.g. *badge*- or biometrics –e.g. an iris scan- which are linked to the different authorizations for different groups; (temporary) employees with different roles and status, third parties and visitors.

An *onion strategy* could be applied in which a person needs to pass several identification levels in the form of external fences and guards, reception and different access controls inside the organization's location depending on the level of security necessary for the asset. Access to high security areas could use *multi-level identification*. [RED05] Dependent on the level of authority necessary for access one or more of the following should be verified; something you *are* -biometrics-, something you *have* -a token- and/or something you *know* -e.g. personal identification number (PIN) or password.

In summary; organizations need to perform identity and access management.

Security organization

The organizational and functional structure should be making it hard -if not impossible- for the social engineer to attain certain information. This can be achieved by for example *segregation of duties* in which every employee performs part of a task and only knows part of the information and none has the complete picture of the necessary information. This makes it necessary for the social engineer to interact with several targets which increases the chance of detection or not attaining the complete picture. This increases the amount of effort and risk for a social engineer and may discourage him or her.

The risk of social engineering can be of influence all through the employment of a person with the organization. Before hiring an employee a *background check* could take place to verify the identity and ascertain he or she does not have a criminal or otherwise suspicious history. [STO02] When signing their contract employees should accept to function according to the security policy and also accept to keep up with changes in policies, this also holds for current employees to maintain there employment. [RED05] Management should support and enforce this strict policy to make it effective. [GUL03]

To verify if an employee is aware of his or her responsibilities and role within the protection of the organizational assets a *test system* can be created virtually or physically. [RED05] Only when passing the test will they retain access to the asset –information or system. This procedure should then also be applied (in a simplified form) for temporary labor. And finally external personnel should be checked by their employer to create security al through the supply chain.

The organizational and functional structure, employment measures and awareness test need to be taken partly to stop the external social engineer by awareness, but also to stop social engineers from becoming part of the workforce and manipulate coworkers, creating a so-called *insider threat*.

Security policy and procedures

A clear *security policy*[9] addressing social engineering is necessary to build the entire security upon. [CAR06] [GRA06] [GRG02] [JON03] [MIT02] [RED05] The social engineering policy contains standards and guidelines according to which the personnel and systems should function to reach an overall security objective; *mitigate the risks of social engineering attacks*. This policy can be used as a reference in the underlying procedures. [GRG02] The security policy should be uniform and clearly defined, documented and maintained, for consistency and maximum effectiveness. It should be available to all employees but shielded from unauthorized access, this can be realized for example by placing it on the organizational intranet. [RED05] [STO02]

Social engineering *security procedures*[10] are the operational translation of the policy set out by management into a practical series of activities, tasks, steps, decisions or processes to achieve a set outcome -in this case the prevention, detection or recovery from a social engineering attack. These procedures form the actual organizational countermeasures based on the security objectives stated by management. Because employees have to follow these procedures they do not need to make decisions on the fly but can follow predefined steps; this decreases the opportunity for a social engineer to manipulate them. [GRG02] This reliance on procedures makes *document control* very important, to review the procedures regularly and keep them up to date.

Mitnick describes a comprehensive –but limited- list of what social engineering security policy and procedures should address. [MIT02] The following table classifies these and policies and procedures from other literature according to the employee group they pertain to or the subject they address:

Classification	Policy/Procedure
Management	• Data classification • Authorization • Authentication • Information disclosure • Phone administration • Incident monitoring
Information technology	• General IT security • Help desk • Computer administration • Computer operations

[9] 'Policy is a deliberate plan of action to guide decisions and achieve rational outcome(s)'. [WIK06]

[10] 'A procedure is a specific series of activities, acts or operations'. [WIK06]

All employees	• General employee security • Computer use • Email use • Phone use • Fax use • Voicemail use • Password • Incident response
Specific employees	• Telecommuter • Human resource • Receptionist • Incident reporting group • External party
Physical security	• General physical security • Security guard

Table 5: Social engineering policy

The policies and procedures by themselves form a basis to build a defense against social engineering attacks on. But when they are not followed strictly this only forms a limited defense. To gain (employee) compliance, management needs to support and enforce these policies and procedures and implement an awareness program to embed the knowledge into the personnel and organization. [GRA02]

Security awareness

The security awareness program should create continuous awareness of the social engineering risk among the organizations employees and their (personal) responsibility in protecting the organization’s assets. [GRA02] [SAG02] The program should consist of (interactive) trainings with clear reference books discussing the security policies and procedures of the organization, the tactics and psychological principles used by social engineers and the targeted information (and value thereof). This *security awareness training* teaches the trainees to recognize an attack when it occurs and prevent it from causing harm by following policy and set procedures. [GRA02] [MIT02] Even if an attack is detected later on, this recognition can help with the recovery. The training should also discuss information and attributes –e.g. uniforms and letterheads- an attacker may already have. This awareness can be used to refute the tendency to trust a person having certain information or attributes. And finally the consequences of an attack to the organization, the organizational environment –e.g. suppliers and clients- and the employee personally should be addressed to generate support for the security architecture.

Next to training on the social engineering attacks employees should also get *technical training* on the information systems they use, to make them aware that the technical security features on these systems do not protect the organization’s assets by themselves and that they should question the credibility of requests for actions on them. [MIT02] [STO02] This increases the chance of detecting illegitimate requests by a social engineer or coworker and recovery from an attack.

The profundity of the training depends on the access rights of the employee –e.g. systems administrators- and level of contact with the public –e.g. helpdesk personnel and receptionists-, but all personnel internal and external –e.g. security guards and cleaners- need to get basic security training on social engineering. [GRG02] Therefore distinct training programs should be created for the different groups, some more focused on the technical systems security, others more on the physical security. [MIT02]

Security culture

The final goal of the awareness program is to create a culture in which security is embedded and employees are constantly aware and conscientious of the social engineering risk. [ALL05] [ALL06] [LAF04] To achieve this *security culture* all personnel should be motivated and see information security as a responsibility and part of their function within the organization. To be willing to help create and maintain the security culture, they need to see the importance for the continuity of the organization and for them individually, as social engineering can endanger the organizations assets, their personal information held by the organization, as well as their future employability within the organization or other organizations. [MIT02] It is therefore important to make employees perceive the risk of social engineering and make them aware of their (personal) responsibility, by for example giving them a reality check by performing a *penetration test* and confronting them with the outcome. [DUD06] [GRG02] [LAB06] [LAF04] [KAN07] [SAG02] This risk perception can support user acceptance and conscientiousness, and therewith support the *security objectives* and efforts of the organization and its stakeholders. [STO02]

Some aspects of this culture:

§ It should have management support; policy and procedures also apply to them, no excuses possible.

§ It should cover all employees and stimulate suppliers and other third parties to do the same to spread the security culture all over the supply chain or network.

§ It should encourage compliance and discourage defiance by reprimanding actions that are in conflict with the security policy and procedures. [JON03]

§ But it should also support not withholding mistakes so (recovery) actions can be taken directly. [CAP06]

§ It could make use of bulletin boards and other media to constantly remind employees of their responsibilities and the dangers of social engineering. [GRG02]

This culture can also lead to the obtainment of a security certification which should be upheld. [CAR06]

Monitoring and evaluation

Risks can change easily through the growing knowledge and ingenuity of social engineers; a hard to attack vulnerability can change into a gaping hole in security by the wide distribution of a simple new exploit -tactic or complete attack- by a social engineer. [EMA05] [ZAG02] Therefore regular *reviews* and *updates* of the controls and measures should be performed. *Monitoring* on incidents and responses is very important to see if there are still cracks in security that need immediate repair or to find trends in attacks. This knowledge can lead to changes in the different controls and should also include changes proposed by personnel and new insights from (security) literature, creating continuous improvement. [RED05]

Next to this continuous process periodic evaluation should take place. The performance of the social engineering security controls can be measured by *periodic audits* on the different controls and measures. [JON03] A tool that is used is a simulation of an attack –*penetration test*- to expose vulnerabilities as well as to maintain consciousness. [ALL06] [LAB06] [MAN06] An organization can furthermore choose to obtain a security certificate and audit this periodically to secure a certain level of security. This creates not only security management but security leadership.

This monitoring, evaluation and improvement process needs continuous management commitment and support to maximize effectiveness. [STO02] [ISA06]

Preconditions

Before implementing the security architecture –controls, policies, standards and procedures- some preconditions have to be fulfilled to make them useful and guarantee maximum success:

§ It should not disrupt day to day operations and needs to be flexible enough to be used in the organization. [ALL05] [ALL06] [LAF04] [STO02] The basic precondition is therefore the creation of a balance between ease of use and level of security.

§ It needs to be able to differentiate between an attack and normal day-to-day activity. [ALL06] It should therefore only generate a minimum of false negatives and false positives.

§ The set of implemented controls, policies, standards and procedures needs to be robust enough to block a variety of malicious actions occurring concurrently or in sequence. [ALL06]

§ The risk management process and implementation of controls needs to have management support and commitment to be a success. [ALL06] [ISA06] [STO02] [RUD04]

This again emphasizes the importance of management all through the information security process and the impact of their choice of controls and countermeasures.

Summary

This chapter discussed the information security controls an organization could implement to solve the problem of social engineering risk.

§ A list of general information security controls is given, classified according to the function of the security control –*general IT*, *prevention, reduction, detection, repression*, *correction* and *evaluation*- and to the level in the organization -*strategic, tactical* or *operational*.

§ Because this thesis focuses on the human factor in information security some important organizational and physical elements of the security architecture have been discussed; *physical security*, *security organization*, *security policy and procedures*, *security awareness program*, *security culture* and *monitoring and evaluation*.

§ And finally some preconditions were given which emphasize the importance of the management commitment and support.

Because of limited budgets organization need to make a choice what they want to secure, against which social engineering attacks and within which time frame to implement the mitigating controls to achieve their security objectives.

To mitigate the risks social engineering imposes on organizations in the long run organizations need to manage these risks. How this management is performed in practice is discussed in the next chapter. This discusses the empirical research performed for this thesis which lead to the current form of the thesis and proposed social engineering risk management model.

‘Unknown risks are accepted risks.’

- Atos Consulting Information Risk Management [ATO06]

Empirical research

One of the elements of the overall research framework -the empirical cycle- consists of observations. [SWA90] These *observations* are part of the empirical research and used to verify the theoretical research and to create a social engineering risk management model in line with the wishes of real-life organizations. [GEU99] In this chapter the empirical research will be discussed, starting with the problem description, followed by the research approach and the findings and conclusions of this empirical research.

Problem description

The problem as defined in chapter 2: ‘Project description’ also set the focus for the empirical research:

> *There are no tools available to measure the risks social engineering imposes on organizations and which countermeasures they can take to mitigate these risks.*

This statement also needs to be verified by the empirical research and practical insights may lead to solutions other than already found in the theoretical research.

The main research questions posed in the same chapter hold in this empirical research.

> 1. *Which risks do organizations run as to social engineering?*
> 2. *Which countermeasures can be taken by an organization to protect themselves against the threats of social engineering?*
> 3. *How can organizations measure the social engineering threat and mitigate the risks it poses?*

These questions also need to be answered from a practical perspective, through research in real-life organizations and situations. The empirical research performed is therefore used to challenge and verify the stated assumptions and hypothesis in the thesis as well as research and findings in studies used to base this theory on. The empirical research together with the theory therefore forms a sound basis to build the model on -questions 1 and 2- and to validate the preliminary steps of a social engineering risk management model -question 3- and its interpretation. The scope of this research will again be on all aspects of influence on social engineering.

Research approach

To answer the research questions and help solve the problem a suitable research strategy needs to be chosen, tailored to this research and finally implemented. There are several ways to perform empirical research; experiments, histories, case studies, surveys and archive analysis. Each of these has their advantages and disadvantages in different situations. The choice of a research strategy therefore depends on three conditions: [YIN03]

§ The kind of research question.

§ The control the researcher has over the actual behavioral events.

§ The focus on contemporary or historical phenomena.

Strategy	Form of research question	Requires control over behavioral events?	Focuses on contemporary events?
Experiment	How, why?	Yes	Yes
History	How, why?	No	No
Case study	How, why?	No	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archive analysis	Who, what, where, how many, how much?	No	Yes/No

Table 6: Research strategy

As the final objective of this empirical research is the validation of the preliminary design and generating requirements the focus is on research question 3, a ‘how’ question. The control over the actual behavior of the organization and its representatives is limited. And the focus is on a real-life organization and contemporary phenomenon. Together with the limited timeframe of the research project, the focus on very specific and in-depth information and the qualitative results, these conditions make *case studies* the most suitable methodology. [VER07] [YIN03]

Case studies

During a case study data is collected, presented and analyzed. [YIN03] This can be performed in several ways. Case studies can be subdivided by the number of cases selected for analysis. Two main forms of collection can be identified: [YIN03]

§ *Single-case study*; focuses on only one case and goes very deep.

§ *Multiple-case study*; focuses on multiple cases which are compared to reach a conclusion, also known as a *comparative case study*.

Because all organizations can be a victim of a social engineering attack the diversity in these organizations needs to be studied. This makes the proposed social engineering risk management model less rigid as it should be helpful to all and not one specific case.

The multiple-case study can again be subdivided into two methods by the moment of analysis: [VER07]

§ *Hierarchical method*; the cases are all studied individually first, followed by a comparing study on all cases.

§ *Sequential method*; first one case is studied, on the basis of the findings another case is chosen en studied, etc.

The sequential method would have made it possible to perfect the model over time, but it would take more time then available and a lot of cooperation of several organizations. Because of a limited timeframe for the empirical research and a limited number and amount of time available at participating organizations the hierarchical method was used. However, insights from each consecutive case have been used to adjust following case studies.

The empirical research was therefore performed through case studies at multiple organizations, with limited intermediate analysis and evolution and a final comparison of the results after all studies were performed. Now that the choice of research is clear the way the information was gathered will be discussed.

Information sources

Yin identifies six sources of information for case studies; documents, archives, interviews, direct observation, participating observation, physical artifacts. [YIN03] Because of the sensitive findings that could come to light, organizations are very protective over information on specific events in their *archives*. They also do not wish to have a graduate *observing* their (critical) activities, which is also very time-consuming. The empirical research therefore focuses on two sources of information the organizations are willing to collaborate in and share; *interviews* and *documents*. The documents can have any form; from factsheets with best (security) practices to entire security policy documents.

For the interview a choice was made between unstructured, semi-structured and structured interviews. [SAU06] [VER07] Because of the broad scope of the subject an *unstructured interview* could lead to long discussions on less relevant matters. A completely *structured interview* eliminates the possibility to go deeper into subjects of great relevance that where not foreseen. Therefore *semi-structured in-depth interviews* were chosen to get founded answers to the specific research questions. [SAU06]

Questionnaire

The interviews were held using a leading *questionnaire* of open questions. An example of the questionnaire can be found in Appendix C: ‘Notes Empirical research’, one original Dutch version and an English translation.

The questionnaire consists of the following stages:

§ *Interview introduction*; consisting of an introduction on the graduation project, the interview and use and confidentiality of the provided information.

§ *Interviewee introduction*; consisting of an introduction to the organization, the function of the interviewee and relevance of this function in the information security within the organization.

§ *Verification definition social engineering*; consisting of stating the definition of social engineering used in the thesis and verifying the knowledge of this phenomenon with the interviewee.

§ *Model walk through*; consisting of a short introduction of the preliminary social engineering risk management model and answering the relevant questions related to the different steps in the preliminary model.

- *Closing*; consisting of the verification of the usefulness of the steps in the preliminary model and possible recommendations, as well as thanking the interviewee for participating in the empirical research.

The questionnaire structures the interview but still makes it possible to go deep enough to answer the research questions with a clear foundation.

Case selection

The interviewed organizations were chosen based on the reliance of their business on information and IT and the level of risk of a social engineering attack. [SAU06] The interviews have therefore been held with an *international IT service organization* [11] because of its business focus on information processing and storage for external parties, a *consulting organization* which greatest assets are its personnel and knowledge, a *regional governmental organization* because of its increased risk to a social engineering attack and finally the *Computer Emergency Response Team* of the Dutch government (GOVCERT) as the focus of this organization is on the cyber security within the government by coordinating IT security incidents, informing and advising on these incidents and supporting the governmental organizations in the prevention of, and response to security incidents. During this interview at GOVCERT both the organization itself as the general view on information security in the Netherlands were discussed

All these organizations have a different perspective on information, its value, the risks they run and possible counter measures. Within the visited organizations the interviews where held with security officers and/or other security responsible personnel. Together these interviews represent a valuable perspective on social engineering as these organizations and specific interviewees should be the ones at the forefront of information protection from for example social engineering. An exemplary interview report is given in Appendix C: ‘Notes Empirical research’.

Seminar

Next to these interviews the opportunity presented itself to present the preliminary research findings during an information security seminar followed by discussion between the security representatives of several governmental organizations (national, municipal and penitentiary), an insurance company and organizers Atos Origin and Atos Consulting. The given introductory presentation can be found in Appendix C: ‘Notes Empirical research’.

Other information sources

During the graduation other opportunities were also created to informally discuss the subject with security responsible persons from for example a knowledge intensive production organization and an organization which handles extremely valuable products. Also seminars where visited and several case studies and research projects had already been studied during the theoretical research,

[11] The organization names cannot be published due to the sensitive nature of the subject and answers.

therefore limiting the number of interviews performed. [JAN05] [KIE06] [KRA05] [RED05] [SPE04}[STE02]

Overall conclusions and recommendations

Based on the interview findings several general conclusions can be drawn and recommendations can be made. To see if the research questions have been answered the conclusions will be summarized according to these:

1. *Which risks do organizations run as to social engineering?*

The organizations can identify social engineering risk when presented with examples and the definition. They also see the necessity of mitigating this risk. A model should therefore be able to help the organization in determining the risk as at this time the organizations still focus on technical and physical risks rather then human based risk and may overlook very important aspects otherwise. The classification of the social engineers, their motives and tactics are identified as very helpful in this.

2. *Which countermeasures can be taken by an organization to protect themselves against the threats of social engineering?*

Most organizations do not have specific countermeasures against social engineering. They however do already have several countermeasures in place against other threats to information or physical security. These countermeasures should be listed and compared to a list of possible social engineering controls, to measure the gap and with that residual risk.

3. *How can organizations measure the social engineering threat and mitigate the risks it poses?*

Organizations have set objectives for their information security. In this they tend to forget or not specify objectives to manage the risk of social engineering which makes it hard to measure this specific risk. This tendency is in part fueled by limited time and budgets, but this should not be an excuse to leave the risks unattended as the consequences to the organization can be great. Therefore organizations should determine the risk of social engineering to their organization and implement mitigating controls if necessary.

To mitigate the risk organizations prefer general information security models over yet another model next to all others. The social engineering risk management model should therefore be able to link to current security processes and models. It could be incorporated in these or could use the knowledge and means already available and form an add-on to the existing processes and models.

A general recommendation in line with these former recommendations is that the model should not be static. Underlying lists with tactics, possible controls, etc. should be updated continuously. And the model should be evaluated and reviewed periodically to see if it still fills the need of organizations in helping them manage their social engineering risk.

Summary

This chapter discussed the empirical research as relevant part of the empirical cycle.

- The research problem for the empirical research was stated, which is the same as that of the overall research project. The problem definition and main research questions are therefore also the same.
- The research approach most fitting was the use of a *multiple-case study*, using the *hierarchical method*. The information for this analysis was sourced using *semi-structured in-depth interviews* lead by a *questionnaire of open questions*.
- And several conclusions and recommendations from the interviewed organizations are stated which set preconditions to the proposed social engineering risk management model.

The findings, conclusions and recommendations have been analyzed and used to review the steps in the preliminary social engineering risk management model leading to the model described in the next chapter.

‘The sciences do not try to explain, they hardly even try to interpret, they mainly make models. By a model is meant a mathematical construct which, with the addition of certain verbal interpretations, describes observed phenomena. The justification of such a mathematical construct is solely and precisely that it is expected to work.’

- John von Neumann, Chaos [NEU44]

Managing social engineering risk

Organizations need to minimize the potential of loss, also known as *risk* to stay in business. [EMA05] [DOP08] Minimize, because risk will always be present regardless of its probability. Organizational security focuses on the reduction and management of this probability by designing and implementing security controls that reduce the risks to an acceptable level. This chapter proposes a risk management model to analyze social engineering risk and manage the security level related to this risk. [RUD04] But first the relevance of this modeling process will be discussed and its relation to Enterprise Risk Management.

Social engineering risk management

Social engineering risk management can be defined as follows: [COS04]

> *Social engineering risk management is a process, influenced by an organizations management and other personnel, applied across the organization, designed to identify social engineering risk and manage this risk to be within the security level, to provide reasonable assurance regarding the achievement of an organizations objectives.*

Organizations can use social engineering risk management in several ways: [COS04]

§ It can help organizations set the security level in line with their (security) strategy.

§ It can help organizations identify and select from different risk responses.

§ It can help identify and manage interrelated risks and the impacts thereof.

§ It can help reduce uncertainty and therefore loss.

To support the management process a social engineering risk management model is proposed. This uses well-known and frequently used models as a basis which makes the final risk management process more transparent and therefore supports the achievement of the organization's objectives now and in the future. This can furthermore lead to efficiency and effectiveness of operations and compliance with laws and regulations. An adaptation of the models has been made to social engineering risk and generalized to be applicable for all information and not only for IT. It however must be emphasized that this risk management model only creates guidance; it *assists* organizations in the management of social engineering risk.

The social engineering risk management model will be discussed after a short introduction to the security models from which it is derived.

Social engineering risk management model

Social engineering risk is only part of an organizations overall risk. The management of it will therefore also be discussed in this light. The proposed social engineering risk management model is based on elements of Enterprise Risk Management Integrated Framework (ERM) of the Committee Of Sponsoring Organizations of the Treadway commission (COSO).

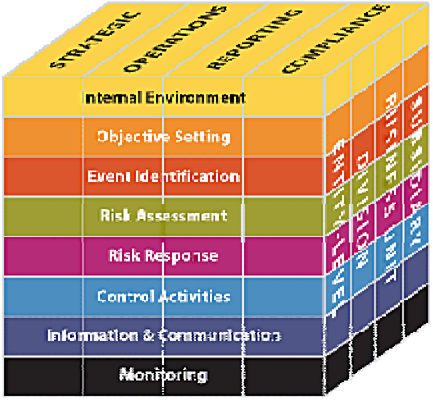


Figure 9: COSO Enterprise Risk Management Integrated Framework

This is used as reference model and specified to social engineering risk. The basic COSO ERM framework is discussed in Appendix D: 'Notes Managing social engineering risk'. The model furthermore uses input from the United States National Institute of Standards and Technology (NIST) risk management guide for information technology systems, IT Infrastructure Library (ITIL) risk management and other literature. [CAZ99] [COS04] [STO02] But it is still described on a high level as there is not 'one' solution for all organizations. [RUD04] References to the rest of the thesis or other literature can be helpful in tailoring the model to the organization, as these provide more specific and in depth analyses and information. Organizations can furthermore choose to model and/or manage their social engineering risk in collaboration with a certified or reputable third party to support them with expertise. [DOP08]

The relevant steps to mitigate and manage the social engineering risk distilled from literature and the empirical research will now be discussed mapped against the components of the management process.

Internal environment

To be able to make a founded assessment of the risks an organization is running it is important to know the organization and its environment.

Step 1: System and environment characterization

In this step the 'system' is characterized in which the social engineering risk needs to be managed. The *system* can be an entire organization, a division, a department, a process or even a specific information system. This is a broader perspective then the *organizational layers* defined in the ERM framework, to be able to get more detail and therefore more specific risk responses if necessary. The characterization therefore sets clear boundaries on the system in scope. [STO02]

The system consists of the organizational processes occurring within this system and the information and data processed by this system. [STO02] This organizational environment in which the personnel operate needs to be described. [COS04] The characterization therefore generates essential information on the system for following steps as well as information on the environment that influences it, for example: [COS04] [LOV05]

General information	System related information
• General organization description • Organizational vision and mission • Organizational objectives • Organizational structure • (Security) culture description • General security policy • General security controls • General security objectives • Human resource policy • Assignment of authority and responsibility	• General systems description • Processes performed by the system • Persons who use the system • Persons who support the system • Available information and data • Available information systems • Available networks • Communication means • System and data criticality • System and data sensitivity • Security policies on system • Security controls on system

Table 7: System related information

This information can be gathered throughout the management process through questionnaires, interviews and document reviewing or -for the technical system information- through the usage of automated scanning tools. [STO02] The risk management process should therefore be seen as an iterative process.

This step yields a characterization of the system, its environment and the boundary between these.

Objective setting

As the system and environment characterization sets the system scope, the process scope should also be set. Therefore the objectives of the social engineering risk management process should be clarified. These can also be used for the evaluation.

Step 2: Objective setting

The ERM framework identifies the organizational objectives in one of its dimensions. The four proposed categories can be divided in strategic and related objectives: [COS04] [CAP06] [RUD04]

§ The *strategic* objectives state high-level goals derived from the organizations vision and mission and state how the management wishes to achieve these. [COS04] The strategy chosen by management is based on a risk assessment similar to the one discussed later on. This yields a *security level* -amount of risk management is willing to take to create value- also known as risk appetite that can be used during the risk response against social engineering risk. [COS04]

More specific formulations of the strategic objectives can be made to support the chosen strategy.

§ *Operations* objectives state the effective and efficient use of the organizations resources. [COS04] Resources are limited and cannot be used both for maximum performance and maximum security. These objectives therefore give insight in the consideration between performance and security and set preconditions on the allocation of resources to stop the social engineer. [EMA05]

- *Reporting* objectives state the reliability of reporting. Internal reporting is important to support management in making decisions and monitoring activities and performance. [COS04] It can furthermore be used as input for external reporting like financial statements. Reporting tools or procedures should therefore be part of the management process.

- *Compliance* objectives state the compliance with applicable laws and regulations. Organizations depend on these and need to adhere to these to stay in business. Compliance objectives therefore set preconditions to the operations in the organization including the security management process.

The strategic, operations and internal reporting objectives are in the range of influence of the organization. The external reporting and compliance objectives however depend on external influence. These objectives are not mutually exclusive as an objective can be related to more categories. [COS04] But all objectives set preconditions on possible choices during the management process. The levels in which the management accepts variation in the achievement of the objectives -*risk tolerance*- creates a playing field in which the management can implement mitigating actions against social engineering risk.

Part of the information should already be available from the environment description and part will come to light during the management process. Management should try and set the scope as clear as possible to support the following steps.

This step yields strategic, operations, reporting and compliance objectives as well as the risk tolerance and appetite related to these.

Event identification

To implement controls first the events need to be identified that could influence the organization. [COS04] As social engineering poses risk and not specific opportunities when doing legitimate business only the negative factor of events -risk- will be discussed. As this risk only exists when there is a treat (event) these will be discussed with the related threat source.

Step 3: Threat identification

Social engineering risk is generated by several threats as visualized in chapter 2: ‘Project description’. Therefore these threats should be identified first. A *threat* is an action or event that might violate the security of an asset. [MAI03] [SWA01] It is caused by a threat-source and violates the security of an asset by exploiting a specific vulnerability in the system. [LAF04] [STO02] This threat can be any application of social engineering tactics or complete attack that compromises the confidentiality, integrity or availability of the organization’s information, information system, network or data.[12] A list of tactics has been given in chapter 4: ‘Social engineering attacks’:

[12] Accidental triggering of a vulnerability will not be discussed further as it does not fall in the scope as stated in Chapter 1: Introduction.

Social engineering tactics	
1. Physical reconnaissance	11. Virtual impersonation
2. People spotting	12. Reverse social engineering
3. Dumpster diving	13. Tailgating
4. Forensic analysis	14. Piggybacking
5. Phreaking	15. Office snooping/Desk sniffing
6. Phishing	16. Item dropping
7. Mail-outs	17. Data leakage
8. Web search	18. Direct approach
9. Profiling	19. Identity theft
10. Physical impersonation	20. Malicious software

Table 8: Social engineering tactics applied

A *threat source* is in case of social engineering a human; any social engineer with intent and motivation. The *intent* may be assumed to be present within all social engineers discussed in this thesis. The possible threat sources are summarized in the following table together with the *motives* of social engineers as discussed in chapter 3: 'Hackers and social engineers':

Threat sources	Social engineer's motives
• Casual social engineer	• Financial gain
• Political social engineer	• Personal interest
• (Organized) criminal	• External pressure
• Internal agent	• Intellectual challenge
	• Damage containment
	• (Personal) grievance
	• Politics

Table 9: Threat sources and social engineer's motives

This step yields a list of threat sources relevant to the organization and system, and properties of these that could be used to exploit a specific vulnerability in the system.

Risk assessment

The possible loss of control caused by social engineering can have serious consequences and organizations therefore need to identify the risks that are relevant to them in line with their general and security objectives. [DOP08] Therefore a clear risk assessment should take place before implementing security controls. [RUD04] This assessment consists of several steps to specify the risks and related variables to determine the influence it could possibly have on the system and organization. On this basis decisions can be made to select proper action.

Step 4: Vulnerability identification

To obtain the desired information the social engineer needs to have *opportunity*; as long as there is no vulnerability to exercise, there is no risk. [LAF04] [STO02] As defined in chapter 2: 'Project description' a *vulnerability* is a flaw or weakness that can be exploited to breach the security of an asset. [VER01]

The social engineers targets people and can use a variety of psychological principles -discussed in chapter 4- to turn the human into a weakness and gateway to information:

Psychological principles
• Strong affect
• Overloading
• Reciprocation
• Deceptive relationships
• Diffusion of responsibility
• Moral duty
• Authority
• Integrity
• Consistency

Table 10: Psychology principles

Every place an employee or other party can obtain access is therefore potentially at risk and creates a vulnerability when this location contains the targeted information. Chapter 4 lists the information a social engineer is likely to target during his or her attack:

Gathered information
a. Organizational structure
b. Employee names
c. Employee functions
d. New employees
e. Calendars
f. Internal phone numbers
g. E-mail addresses
h. Organizational policy and processes
i. Lingo
j. IT infrastructure
k. Organizational logos
l. User names
m. Passwords
n. Server names
o. Application names
p. Manuals
q. IP addresses

Table 11: Information gathered and used in social engineering attacks

Organizations need to localize this information within the organization to list possible targets of the social engineer.

Furthermore information specific to the organization and its environment needs to be examined to identify specific threat sources and vulnerabilities. This information can be gathered through reviews of the systems history -e.g. previous risk assessments on social engineering or other information risks, security violations and incident reports-, security control reviews and interviews with personnel -specifically system administrators and helpdesk personnel. [STO02]

Another way of obtaining insight in possible vulnerabilities is testing. Security testing and evaluation consists of the creation and execution of a test plan which tests the operational effectiveness of current controls and policies. [STO02] A very specific test method is *penetration testing*, during which an attempt is made to circumvent the system security from the viewpoint of the threat source -the social engineer- to expose possible vulnerabilities of the system, controls, procedures, etc. [ALL06] [LAB06] [MAN06]

This step will yield a list of system and organizational vulnerabilities a threat source could exploit.

Step 5: Control analysis

An organization will have implemented several controls for information security, specifically against social engineering or against other threats like the hackers or its own personnel. These current controls and future planned controls need to be listed and classified according to their level in the organization *-strategic, tactical* or *operational-* as well as their control category *–general IT*, *prevention, reduction, detection, repression*, *correction* and *evaluation*. Comparing this list with the following control checklist from chapter 5: 'Stop the social engineer' gives a clear view on the present level of security on the system and its environment:

Classification		Control
General	Strategic	Security culture Security policy Ongoing risk management
	Tactical	User awareness procedures Data classification procedure
	Operational	Security awareness and technical training Data classification Segregation of duties Basic identification measures System protection features Key management
Preventive and reductive	Strategic	Risk assessment Security documentation and planning Security responsibility assignment Personnel security
	Tactical	Authentication procedure Authorization procedure Data media usage Non-repudiation Protected communication measures Transaction privacy measures
	Operational	Access control enforcement Data labeling and distribution Malicious software prevention Offsite storage Facilities safeguarding Physical systems protection
Detective and repressive	Strategic	Audit policy
	Tactical	Incident response procedure Periodic control review Periodic audit
	Operational	Internal & external audits Intrusion detection Malicious software detection Incident response Intrusion containment
Correction	Strategic	Recovery policy

	Tactical	Backup procedures Recovery procedures Disaster recovery plan
	Operational	Security state restoration Malicious software removal
Evaluation	Strategic	Ongoing risk management
	Tactical	Logging procedures Evaluation procedures Non-repudiation
	Operational	Logging activities Security documentation

Table 12: Social engineering controls

This gap analysis identifies potential system, process and procedural vulnerabilities that are not yet addressed. [STO02] This vulnerability analysis together with the threat identification can be used to maximize benefit from the implemented controls. [MAN06]

This step yields a list of current or planned controls for the system and entire organization to mitigate the social engineering risk.

Step 6: Likelihood determination

The difficulty in exploiting a vulnerability is a combination of the expertise required, available tactics, the ease of use of these and the relative exposure of the vulnerability. [INS06] Which tactics will be used by a social engineer therefore depends on the vulnerability they can exploit and the risk they are willing to run. To determine the likelihood of a threat occurring, an estimate has to be made of 1) the threat sources motivation and capabilities, 2) the nature of the vulnerabilities and 3) the existence and effectiveness of current controls. [STO02]

The motivation of the social engineer has already been identified during the threat identification. But the *capability* has not been discussed yet as it cannot be completely related to the threat sources as -next to the expertise- the access, means of interaction and boldness of the social engineer all influence the risk to the social engineer and therefore the necessity of expertise to lower this risk.

- The *expertise* of the social engineer consists of knowledge and skills. The different tactics a social engineer can use -as discussed in chapter 4: ‘Social engineering attacks’- need different knowledge -based on experience and preparation- and skills of the social engineer.

- The *access* depends on the origin of the social engineer, *inside* -employees or trusted third parties- or *outside* the organization -external parties. Both insiders and outsiders can use the same tactics. Albeit that the insider has a great advantage by obtained trust. This lowers risk of getting caught, but may increase the consequences for the social engineer when caught exponentially.

- The amount and means of *interaction* of the different social engineering tactics also influence the risk, as more interaction means a higher chance of getting caught. [INS06]

§ The *boldness* of the social engineer will finally determine if and which tactic will be used and how much risk the social engineering is willing to run to reach the goal of the attack.

Setting aside the boldness of the social engineer the different tactics need a different skill level of the social engineer. As the skill level increases the social engineer will be more willing to take risks to gain greater benefit. The tactics as discussed in chapter 4 are summarized in the following table according to the expertise level of the social engineer and the means of interaction[13]. The expertise level runs from *low* -for easy to use tactics which do not need much preparation or even social or technical skills- to *high* -for attacks which need substantial social and/or technical skills. The interaction can be classified as *none* (*existent*), *virtual* -using a medium- or *physical* -on location/in person.

Expertise level of social engineer	Means of interaction	Social engineering tactics
Low	None	• Physical reconnaissance • People spotting • Dumpster diving • Web search
	Virtual	• Virtual impersonation
Medium	None	• Forensic analysis • Phreaking • Profiling
	Virtual	• Mail-outs • Phishing • Reverse social engineering • Malicious software
	Physical	• Direct approach • Tailgating • Piggybacking • Office snooping/Desk sniffing • Item dropping
High	Virtual	• Identity theft
	Physical	• Physical impersonation • Data leakage

Table 13: Capability classification social engineering tactics

In summary threats can be classified according to the general source and more specific motivation of the social engineer as well as to the capabilities this social engineer will need to have to apply specific tactics. The vulnerabilities and current controls generated during the vulnerabilities identification and control analysis complete the input for likelihood determination.

[13] When tactics fit several categories they are categorized in the lowest skill level group.

The NIST identifies three likelihood levels: [STO02]

Likelihood level	Likelihood definition
High	The threat source is highly motivated and sufficiently capable and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat source is motivated and capable, but controls are in place that may mitigate successful exercise of the vulnerability.
Low	The threat source lacks capability or controls are in place to prevent the vulnerability from being exercised.

Table 14: Likelihood level of social engineering attack

If necessary more or other levels could be implemented or its definition could be changed.

This step yields a likelihood rating of a vulnerability being exercised by a social engineer.

Step 7: Impact analysis

The definition of social engineering already implies the risks of social engineering. A social engineering attack can potentially lead to the loss of control over information, an information system, network or data by compromising the confidentiality, integrity or availability: [DUD06] [MAI03] [STA02] [SWA01]

§ *Confidentiality* is upheld when the information is secret and only accessible to authorized persons.

§ *Integrity* means the information and data is correct and not manipulated by an unauthorized person.

§ *Availability* refers to the fact that information, information systems, networks or data are accessible, next to the applications that perform operations on them.

The confidentiality can be compromised by possible unauthorized *disclosure*, the integrity by possible unauthorized, unanticipated or unintentional *modification* and the availability can be compromised by possible unauthorized *modification, relocation* or *deletion*. [RUS02] [SWA01] As soon as information, an information system, network or data may have been compromised the *possibility* of this access or distribution, modification and deletion already means a loss of control over the asset.

Organizations therefore need to asses the impact of loss of either of these security goals. [STO02] The sensitivity and criticality of the information, an information system, network or data is therefore needs to be defined.

The NIST identifies three impact levels: [STO02]

Impact level	Impact definition
High	Exercise of the vulnerability may result in highly costly loss of assets or resources, significantly harm the organizations mission or reputation or lead to serious injury or death.
Medium	Exercise of the vulnerability may result in costly loss of assets or

	resources, harm the organizations mission or reputation or lead to injury.
Low	Exercise of the vulnerability may result in some loss of assets or resources or noticeably affect the organizations mission or reputation.

Table 15: Impact level of social engineering attack

If necessary more or other levels could be implemented or its definition could be changed.

This step yields an impact rating of a vulnerability being exercised by a social engineer.

Step 8: Risk determination

The risk assessment ends with the determination of the risk an organization is running. To determine which risks are most eminent and need to be mitigated the likelihood of a threat occurring, the impact of this occurrence and effectiveness of current and planned controls need to be summarized. To make found decisions on which risks to tackle the NIST proposes a multiplication of the likelihood level and impact level according to the following matrix: [STO02]

Likelihood	Impact		
	High	Medium	Low
High	High	Medium	Low
Medium	Medium	Medium	Low
Low	Low	Low	Low

Table 16: Risk level matrix

The three risk levels could be defined as follows:

Risk level	Action description
High	If a system is evaluated at high risk measures should be planned and implemented as soon as possible.
Medium	If a system is evaluated at medium risk measures should be planned and implemented over time.
Low	If a system is evaluated at low risk management or responsible personnel should decide whether to implement measures or accept the risk.

Table 17: Risk level on system or organization

The risks that are tagged to be acted upon go to the next component of the management process in which proper response will be taken.

This step yields a social engineering risk rating of a specific system or entire organization.

Summary

The risk assessment consists of the vulnerability identification, control analysis, likelihood determination, impact analysis and leads to a risk determination in which the most eminent risks are identified. For social engineering this proposed assessment is performed using a qualitative methodology as for most risks there is no quantitative measure.

Risk response

Now the management will need to make a choice on possible actions they will take against the relevant social engineering risks.

Step 9: Risk response

Management can act on the impact and/or likelihood of the risks based on a consideration of costs and benefits. [COS04] These responses -set of controls- depend on the objectives the risks influence and should be within the risk tolerance identified during the objective setting. Management can choose the following responses: [COS04] [EMA05] [STO02]

§ *Risk assumption;* not acting on impact or likelihood, just accepting certain risk.

§ *Research and acknowledgement;* acknowledging the vulnerability and researching possible controls, therefore postponing the actual response.

§ *Risk avoidance;* eliminating the risk cause and/or consequence -vulnerability- by for example changing procedures and practices.

§ *Risk transference;* reducing the likelihood and/or impact by transferring, sharing or compensating (part of the) risk by for example outsourcing services or insuring against specific damage.

§ *Risk limitation;* reducing the risk likelihood and/or impact by implementing controls.

§ *Risk planning;* manage the risk by planning actions to mitigate the risks by prioritizing, implementing and maintaining controls

All these ways of dealing with risk have one or another form of management in it. Risk planning will most probably lead to the best mitigation, but is also probably most costly.

Management needs to evaluate the possible responses to determine which is best suitable to reach the organizational objectives. The following variables could be used for the evaluation and comparison of the possible responses: [COS04]

§ The effect on the already determined *risk level* derived from the likelihood and impact of the threat of social engineering being exercised on a specific vulnerability, therefore influencing benefit.

§ Because of scarce resources limited *costs* should lead to great *benefit*. These costs and overall benefits should therefore be assessed per risk response.

- The possible positive or negative effects of the response on the rest of the organization -*portfolio view*- should also have its influence on the choice of response. This could for example be the innovativeness of the solution or the possible creation of new vulnerabilities. [COS04]

This step yields the responses which give the greatest benefit, at the lowest cost within the risk tolerance.

Step 10: Control implementation

The set of controls constituting the response will now have to be implemented. The NIST proposes an approach for implementation of the risk management controls which can also be adapted to social engineering risk. It consists of seven steps: [STO02]

1. *Prioritize actions* based on the risk level determined in the risk assessment.
2. *Evaluate recommended control options* by analyzing the recommended controls on feasibility and effectiveness to minimize the social engineering risk.
3. *Analyze the cost-benefit* to identify the most economic controls in terms of cost-effectiveness.
4. *Select the specific controls* that will form the social engineering risk response within the set boundaries of objectives and risk tolerance.
5. *Assign responsibility* to appropriate internal or external personnel to implement the controls correctly.
6. *Develop an action plan* to summarize the previous information and add relevant information on the actual implementation project, for example a start and target completion date.
7. *Actual control implementation*

This step leads to the implementation of actual controls constituting the social engineering risk response.

Step 11: Residual risk evaluation

The implementation of controls will probably leave a *residual risk* after implementing the response actions. An assessment of this residual risk has to be made to determine if additional controls need to be implemented to address the residual risk. [STO02]

The risk response process -response determination, control implementation and risk evaluation- should therefore be an *iterative process* to minimize residual risk with limited resources and still support the organizational objectives. [EMA05] [STO02]

This step leads to the optimization of the risk response

Control activities

Control activities play a relevant role to stay in control of the social engineering risk in the future.

Step 12: Supporting policy and procedures implementation

The control activities consist of a set of specific controls namely the *policy* and *procedure*, to state what should be done and how it should be done. These control activities are implemented to ensure that the implemented risk response and underlying controls are adhered to. [COS04] They are in part related to the choice of response, but in general form a backbone for the entire security management of the organization and are therefore applicable to all responses.

Some policies and procedures have already been listed in chapter 4. The following table classifies these according to the employee group they pertain to or the subject they address: [MIT02]

Classification	Policy/Procedure
Management	• Data classification • Authorization • Authentication • Information disclosure • Phone administration • Incident monitoring
Information technology	• General IT security • Help desk • Computer administration • Computer operations
All employees	• General employee security • Computer use • Email use • Phone use • Fax use • Voicemail use • Password • Incident response
Specific employees	• Telecommuter • Human resource • Receptionist • Incident reporting group • External party
Physical security	• General physical security • Security guard

Table 18: Social engineering policy

This step yields a list of relevant policies and procedures related to social engineering risk.

Information and communication

To help personnel and management in fulfilling their responsibilities they need information. They need information relevant to them, in a useable form and in a timely fashion. [COS04]

Step 13: Information and communication management

To manage the social engineering risk management process relevant information needs to be identified, captured and communicated. It is important to do this in all layers of the organization to be able to identify, assess and respond to threats and have a means of communicating relevant information to the management. With this information management can make informed and sound decisions in light of the organizational objectives. [COS04] The quality and timeliness of the information depends on the risk tolerance set by these objectives and the criticality of the risk. The information can have many sources -internal, external, manual and computerized- and forms - quantitative and qualitative.

The communication can also be internal or external, specific to part of the organization or to the entire organization and can use many communication means. [COS04]

Organizations need to assess their information need in relation to social engineering risk and manage the flow of relevant information through the organization to support the achievement of the social engineering risk management objective; to stop the social engineer.

This step yields an overview of information and communication variables relevant to the objective.

Monitoring

Organizations and environments change over time. For example social engineers will learn new tricks and render implemented controls useless. Therefore the effectiveness of the risk management process and underlying controls need to be assessed and reviewed over time. This can lead to new analysis and possibly changes in for example risk response. The assessment can have the form of ongoing and/or periodical evaluation of the social engineering risk management process. [COS04]

Step 14: Ongoing monitoring

In everyday activities monitoring should take place to ensure timely response to social engineering threats and changes in the organization and environment. As this monitoring is ongoing and takes place all over the organization the personnel or monitoring systems can identify and directly react on changes. [COS04] For social engineering it is therefore important that all personnel is trained and aware of possible social engineering attacks so they can all monitor their daily activities for possible new vulnerabilities, upcoming threats or actual attacks. The findings from this monitoring can be reported in the routine reports to inform relevant persons or in case of an incident through an incident procedure and can lead to a review of implemented controls.

This step leads to constant monitoring and if necessary update of the implemented controls.

Step 15: Periodic evaluation

The more structured the monitoring system is, the less relevant periodic evaluations are. But it is advised to still perform periodically evaluation of the system or entire organization to gain maximum assurance. [COS04] This evaluation can for example be an internal or external audit but can also consist of a penetration test of the critical systems followed by necessary changes.

The scope and frequency of an evaluation depends on the determined risk level and system criticality in light of the organizational objectives. Clear documentation of these objectives is therefore important to form a benchmark against which the practical implementation of controls can be measured. This can have the form of a gap analysis as performed in the control analysis step.

It can also be performed against the Control Objectives for Information and related Technology (COBIT). This is a more specific interpretation of the COSO framework into relevant controls. COBIT is however focused on governance of IT but several of its controls also apply to social engineering risk. The management can therefore create a set of social engineering risk management controls in line with the COBIT control framework to support the evaluation. Controls can also be set by the auditor to comply with certain regulations or legislation. The reports can therefore also be for internal or external use.

This steps leads to management or external assurance of control over social engineering risk.

Summary

This chapter discussed the social engineering risk management using a model in line with Enterprise Risk Management (ERM).

§ The chapter started with the definition of social engineering risk management and its relevance and benefits to organizations; the limitation of social engineering risk in accordance with the organizations objectives.

§ Also the goal of implementing a social engineering risk management model based on existing risk management models is stated; to *assist* the organization in managing the social engineering risk.

§ The actual social engineering risk management model structures the risk management process and generates assurance for the management on their level of control over social engineering. It consists of 15 steps; *system and environment characterization, objective setting, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, risk response, control implementation, residual risk evaluation, supporting policy and procedures implementation, information and communication management, ongoing monitoring* and *periodic evaluation*.

§ These steps can be related to the management process components of the Enterprise Risk Management Integrated Framework (ERM) of the Committee Of Sponsoring Organizations of the Treadway commission (COSO) and therefore be implemented as part of this overall management process. The components are; *internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication* and *monitoring*.

This model is fairly elaborate and should be tailored to the organization and/or incorporated in the organizations ERM process.

Based on this social engineering risk management model and the observations from the empirical research conclusions have been drawn and stated in the next chapter.

‘To succeed, jump as quickly at opportunities as you do at conclusions.’

- Benjamin Franklin

Conclusions and recommendations

The project started with a problem that needed attention. Now the research has been performed an evaluation on the objectives and deliverables can be made. In this chapter the conclusions are drawn on the research project, followed by recommendations for further research.

Conclusions

To solve the research problem three main research questions where stated, the deliverables related to these questions will now be discussed to see if the research questions have been answered:

1. Which risks do organizations run as to social engineering?

To be able to identify social engineering risks the definition of social engineering is given in the introduction. Based on the knowledge gained in chapter 3: 'Hackers and social engineers' and chapter 4: 'Social engineering attacks' a risk assessment can be made. This first chapter gives a description of the social engineer comparison to the better known technical hacker. The second chapter states the structure of an attack, including the applied tactics and targeted information.

As this *risk assessment* should be performed structurally this is also a component of the social engineering risk management model as discussed in chapter 7: 'Managing social engineering risk'. When an organization follows the steps in this model and more specifically the risk assessment this will help them to get a view on their specific social engineering risk. It however cannot give a general risk level, because of the great diversity in organizations.

2. Which countermeasures can be taken by an organization to protect themselves against the threats of social engineering?

The information security controls related to social engineering as well as specific controls pertaining to the human factor in information security are discussed in chapter 5: 'Stop the social engineer'. The specific controls are more elaborately discussed because these are more relevant, and the other information security controls are generally known within the organizations.

The *analysis of controls* is a single step in the social engineering risk management model during which the current and planned controls in the entire organization are listed using the lists generated and discussed in chapter 5.

3. How can organizations measure the social engineering threat and mitigate the risks it poses?

The social engineering risk management model as proposed in this thesis can assist organizations in measuring, mitigating and managing the social engineering risk. As it is based on the more general and well known Enterprise Risk Management Integrated Framework (ERM) of the Committee Of Sponsoring Organizations of the Treadway commission (COSO) it has a recognizable structure. When organizations have already implemented ERM, the social engineering risk management model can be seen as an add-on. Otherwise it can be a first start in leading the organization to ERM. But it should not be forgotten that this model only gives guidance and assistance in managing the social engineering risk; the real work still needs to be done by the organization!

In summary the conclusion can be that the social engineering risk management model could solve the research problem:

> *There are no tools available to measure the risks social engineering imposes on organizations and which countermeasures they can take to mitigate these risks.*

The model is however still defined on a high-level and application in practice should show the actual usefulness. On this some recommendations for further research are stated next.

Recommendations

Because of limited time and resources some things did not get into scope for this thesis. Therefore this chapter lists some recommendations for future research on social engineering and related topics.

Evolution

Because the field of social engineering is constantly evolving and the applied tactics are only limited by the social engineers imagination new tactics can be created. [LAF04] [CAP06] The proposed list of social engineering tactics is therefore based on the current situation and will need to be kept up to date by regular updates.

Detailed risk management model

As already stated before, the proposed social engineering risk management model is still described on a high level. However important the management of social engineering risk to organizations, it was to elaborate to discuss completely in this thesis and therefore a more tailored version of the general model fell outside the scope of this project. This more specific model should give the organization the means to support business continuity by better securing their assets through founded decision making, justifiable risk budgeting and clear documentation. [STO02] But it will probably not be possible to make a detailed model that will fit all organizations. It however may be possible to make a general model per industry.

Specific controls

The COSO ERM framework and the social engineering risk management model are not specific enough to give complete insights into possible controls an organization could implement. However the Control Objectives for Information and related Technology (COBIT) model provides a framework for risk management and control based on the COSO components. It is focused on governance of IT but entails many controls which also apply to the mitigation of other information risks like social engineering. Also specific controls focusing on social engineering could be formulated, but this is outside the scope of this thesis. This could also form the basis for a social engineering audit using knowledge gained in this research.

Research and test agreement

Before starting any research on social engineering within an organization clear boundaries should be set to how deep this research may go and how far testers can go when social engineering personnel. Another very important subject is what should be done with the classified information that is generated. Therefore a challenge also lies in the structuring of an agreement process before research and for example a penetration test can be performed.

Overall

In general all controls and tools mentioned in this thesis should be elaborated and molded into practical tools, for the security officer, management and other personnel.

‘Follow effective action with quiet reflection. From the quiet reflection will come even more effective action.’

- Peter F. Drucker

Bibliography

Endnotes

[ACK81] Ackoff, R.L., *The art and science of mess management.* 1981, Interfaces 7p.

[ALL05] Allan, A., K. Noakes-Fry, and R. Mogull, *Management update: How businesses can defend against social engineering attacks,* in InSide Gartner. 2005, Gartner Research: Stamford. xxi: 5p.

[ALL06] Allen, M., *Social engineering*, in *GSEC practical assignment*. 2006, SANS Institute: Washington. 13p.

[AIC05] Australian Institute of Criminology, *Hacking motives*. 2005, Australian Institute of Criminology: Canberra. 2p.

[ATO06] Atos Consulting. *Information Risk Management*. 2006, Atos Consultancy: Utrecht. 2p.

[BEA04] Bearman, R., *A guide to social engineering*, in *Network Security Forum*. 2004, Network Security Technology: Waco. 6p.

[CAP06] Capgemini, *Informatiebeveiliging: Dweilen met de kraan open*. 2006, Capgemini: Utrecht. 3p.

[CAR06] Carey, A., *2006 Global information security workforce study*. 2006, IDC: Framingham. 29p.

[CAZ99] Cazemier, J.A., P.L. Overbeek, and L.M.C. Peters, *Security Management: IT Infrastructure Library*. 1999, Her Majesty's Stationary Office: Norwich. 124p.

[CIA00] Cialdini, R.B., *Influence: Science and practice*. 4th ed. 2001, Allyn and Bacon: Boston. x, 262p.

[COL05] Cole, E. and S. Ring, *Insider Threat: Protecting the enterprise from sabotage, Spying, and Theft*. 2005, Syngriss: Rockland. 350p.

[COS04] COSO, *Enterprise Risk Management - Integrated Framework*. 2004, Committee Of Sponsoring Organizations of the Treadway commission: Altamonte Springs. 16p.

[DOP08] Dopmeijer, S., *Opleiding Audit, Risk, Informatiebeveiliging; Risicomanagement.* 2008, Atos Consulting: Utrecht. 20p.

[DOL04] Dolan, A., *Social engineering*, in *GSEC practical assignment*. 2004, SANS Institute: Washington. 15p.

[DUC04] Du Croix, A., *Project plan: Cost transparency in market oriented IT services*. 2004, University of Twente: Enschede. 21p.

[DUD06] Dudek, L.C. and L.K. Ruffin, *Social engineering & internal/external threats*. 2006, United States Department of the Interior: Washington. 70p.

[EMA05] Enterprise Management Associates, *The metrics of IT risk: Keys to security and compliance management*. 2005, Enterprise Management Associates: Boulder. 9p.

[GEU99] Geurts, P., *Van probleem naar onderzoek*. 1999, Coutinho: Bussum. 191p.

[GRA01] Granger, S. *Social engineering fundamentals, part I: Hacker tactics*. 2001, Infocus. 3p.

[GRA02] Granger, S. *Social engineering fundamentals, part II: Combat strategies*. 2002, Infocus. 3p.

[GRA06] Granger, S. *Social engineering reloaded*. 2006, Infocus. 5p.

[GRG02] Gragg, D., *A multi-level defense against social engineering*, in *GSEC practical assignment*. 2002, SANS Institute: Washington. 21p.

[GUL03] Gulati, R., *The threat of social engineering and your defense against it*, in *GSEC practical assignment*. 2003, SANS Institute: Washington. 13p.

[HAN03] Hansche, S., J. Berti, and C. Hare, *Official (ISC)² guide to the CISSP exam*. 2003, Auerbach Publications: Boca Raton. xxiii, 910p.

[HED93] Hedrick, T.E., L. Bickman, and D.J. Rog, *Applied research design: a practical guide*. 1993, Sage Publications: Newbury Park. x, 141p.

[HIC04] Hicks, M.J., *Problem solving and decision making: hard, soft and creative approaches*. 2nd edition 2004, Thomson: London. xiii, 427p.

[HIN05] Hintzbergen, J. and G.-J. v.d. Ven, *Onderzoek informatiebeveiliging bij Nederlandse organisaties 2005*. 2005, Capgemini: Utrecht. 11p.

[INS06] BT INS, *Ethical hacking threat report*, in *Global e-review*. 2006, BT INS: Mountain View. 17p.

[ISA06] ISACA, *2006 CISA review course: Chapter 5 Protection of information assets*. 2006, Information Systems Audit and Control Association: Rolling Meadows. 115p.

[ISC06] (ISC)², *People and processes more important than technology in securing the enterprise, according to global survey of 4,000 information security professionals*. 2006, (ISC)²: Palm Harbor. 5p.

[JAN05] Janssen, D., *Het versterken van de zwakste schakel in de informatiebeveiliging*, in *Nijmeegs Instituut voor Informatica en Informatiekunde*. 2005, Radboud Universiteit: Nijmegen. 118p.

[JON03] Jones, C., *Social engineering: Understanding and auditing*, in *GSEC Practical Assignment*. 2003, SANS Institute: Washington. 18p.

[KAN07] Kanters, F., *Misleiding als vak: Informatiebeveiliging in de praktijk getest* in *IT Beheer Magazine*. 2007, SDU Uitgevers, Den Haag. 4p.

[KIE06] Kieskamp, A. and R. Smit, *De bouwstenen van social engineering*, in *Nijmeegs Instituut voor Informatica en Informatiekunde*. 2006, Radboud Universiteit: Nijmegen. 96p.

[KRA05] Kratt, H., *The inside story: Disgruntled employee gets his revenge*. 2005, SANS Institute: Washington. 57p.

[LAB06] Labruyere, H., *Mysterieuze gast over de vloer: Vooropgezette incidenten werken.* 2006, Infosecurity.nl. 3p.

[LAF04] Lafrance, Y., *Psychology: A precious security tool*, in *GSEC practical assignment*. 2004, SANS Institute: Washington. 27p.

[LOV05] Loveless, M., *Internal security threats: Identification & mitigation*. 2005, BindView Corporation :San Felipe. 8p.

[MAN06] Mann, I. and L. Allison, *Hacking the human: An introduction to social engineering*. 2006, ECSC: Bradford. 13p.

[MAI03] Maiwald, E., *Network security: A beginner's guide*. 2003, McGraw-Hill Osborne Media: San Francisco. 496p.

[MEL06] Melville, H., J. Bryant, and H.S. Springer, *Moby Dick*. 2006, Pearson Longman: New York. 688p.

[MIC06] Microsoft Corporation, *How to protect insiders from social engineering threats: Midsize business security guidance*. 2006, Microsoft Corporation: San Francisco. 33p.

[MIT02] Mitnick, K.D. and W.L. Simon, *The art of deception: controlling the human element of security*. 2002, Wiley: Indianapolis. xvi, 352p.

[MIT06] Mitnick, K.D. and W.L. Simon, *The art of intrusion: The real stories behind the exploits of hackers, intruders, & deceivers*. 2006, Wiley: Indianapolis. xvii, 270p.

[NEU44] Von Neumann, J. and O. Morgenstern, *Theory of games and economic behavior*. 1944, Princeton university press: Princeton. xviii, 625 p.

[ORG04] Orgill, G.L., et al. *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems*. in *October 2004 proceedings of the 5th Conference on Information Technology Education.* 2004, SIGITE: Salt Lake City. 4p.

[PRO06] Promisec, *Mitigating the internal security threat*. 2006, Promisec: Rishon Le-Zion. 25p.

[RED05] Redmon, K.C., *Mitigation of social engineering attacks in corporate America*. 2005, East Carolina University: Greenville. 6p.

[ROB02] Robinson, S.W., *Corporate espionage 101*, in *GSEC practical assignment*. 2002, SANS Institute: Washington. 10p.

[ROG02] Rogers, M., *A new hacker taxonomy*, in *Department of psychology*. 2002, University of Manitoba: Manitoba. 18p.

[RUD04] Rudd, C., *An introductory overview of ITIL*. 2004, *it*SMF Ltd: Earley. 41p.

[RUS02] Russel, C., *Security awareness: Implementing an effective strategy*, in *GSEC practical assignment*. 2002, SANS Institute: Washington. 14p.

[SAU06] Saunders, M. and P. Lewis, *Research methods for business students*. 4th ed. 2006, FT Prentice Hall: Harlow. Xxvii, 624p.

[SCH06] Schumacher, M., *Security patterns: Integrating security and systems engineering*. 2006, John Wiley & Sons: Chichester. xxxiii, 565p.

[SPE04] Spee, A.J.A.M., *Insider threat in IT*, in *IT Auditing*. 2004, Erasmus University: Rotterdam. 40p.

[STA02] Starreveld, R.W., van Leeuwen, O.C. and van Nimwegen, H., *Bestuurlijke informatievoorzieining deel 1.* 2002, Stenfert Kroese: Leiden. 910p.

[STE02] Stevens, G., *Enhancing defenses against social engineering*, in *GSEC practical assignment*. 2002, SANS Institute: Washington. 10p.

[STO02] Stoneburner, G., A. Goguen, and A. Feringa, *Risk management guide for information technology systems*, in *Computer security*. 2002, National Institute of Standards and Technology: Gaithersburg. 41p.

[SUN98] Sun, T., *Art of war*. 2005, Shambhala Publications: Boston. 224p.

[SWA01] Swanson, M., *Security self-assessment guide for information technology systems*, in *Computer security*. 2001, National Institute of Standards and Technology: Gaithersburg. 95p.

[SWA90] Swanborn, P.G., *De probleemstelling: Een pleidooi voor duidelijke taal.* 1990, Sociologische gids. XXXVII(2): p.107-123.

[THI02] Thiadens, T., *Beheer van ICT-voorzieningen; Infrastructuren, applicaties en organisatie*. 2002, Academic Service: Schoonhoven. 406p.

[VER01] Veríssimo, P. and L. Rodrigues, *Distributed systems for system architects: Advances in distributed computing and middleware.* 2001, Kluwer

Academic: Boston. xxii, 623p.

[VER07] Verschuren, P.J.M., J.A.C.M. Doorewaard, and H. Doorewaard Doorewaard, H. and P.J.M. Verschuren, *Het ontwerpen van een onderzoek*. 2007, Lemma: Utrecht. 330p.

[WIN95] Winkler, I.S. and B. Dealy. *Information security technology?...Don't rely on it: A case study in social engineering*. in *Proceedings of the fifth USENIX UNIX Security Symposium*. 1995, USENIX: Salt Lake City. 5p.

[YIN03] Yin, R.K., *Case study research: design and methods*. 2003, Sage: Thousand Oaks. 182 p.

[ZAG02] Zager, M., *Who are the hackers?* 2002, Infosec News. 3p.

Websites

[RAY03] Raymond, E.S., *Jargon dictionary.* 2003.

Available from: http://catb.org/~esr/jargon/.

[KEY06] Key Skills ILX. *A quick view of PRINCE2*. 2006.

Available from: http://www.prince2.com/p2structure.html.

[USS06] United States Secret Service. *National Threat Assessment Center - Insider Threat Study*. 2006.

Available from: http://www.ustreas.gov/usss/ntac_its.shtml.

[WEB04] Webopedia. *Social Engineering*. 2004.

Available from: http://www.webopedia.com/TERM/s/social_engineering.html.

[WIK06] Wikipedia, *Social Engineering, Phishing, Policy, Procedure*. 2006.

Available from: http://en.wikipedia.org.

References

Arthurs, W., *A proactive defense to social engineering*, in *GSEC practical assignment*. 2001, SANS Institute: Washington.

Capgemini, *Integrated security infrastructure*. 2004, Capgemini: Utrecht.

Carey, A., *2004 Global information security workforce study*. 2004, IDC: Framingham. 30p.

Carey, A., *2005 Global information security workforce study*. 2005, IDC: Framingham. 28p.

Gleick, J., *Chaos: making a new science*. 1987, Viking: New York. xi, 352 p.

De Haas, J., *Hightech crime: Meer blauw op de digitale snelweg.* 2005, Informatie.nl. 6p.

Heerkens, H., *Methodologische checklist*. 2004, University of Twente: Enschede.

Janssen, D., *Plan van aanpak: Het versterken van de zwakste schakel in de informatiebeveiliging*. 2005, Radboud Universiteit: Nijmegen. 20p.

Kieskamp, A. and R. Smit, *Plan van aanpak: De bouwstenen van Social Engineering*. 2006, Radboud Universiteit: Nijmegen. 16p.

Schneier, B., *Secrets and lies: Digital security in a networked world*. 2000, John Wiley: New York. xv, 412p.

Swanborn, P.G., *Methoden van sociaal-wetenschappelijk onderzoek: Inleiding in ontwerpstrategieën*. 1981, Boom: Meppel. 412p.

TSM Business School, *De Algemene Bedrijfskundige Probleemaanpak*, TSM Business School: Enschede. 134p.

Appendices

Appendix A: Notes Project description

The theoretical background will be discussed in this appendix. A variation on the *empirical cycle* by Geurts has been used as a base for the project and elements from PRINCE2 were taken. These will be discussed here along with Swanborn and the *risk analysis* model suggested by Du Croix.

Geurts

In his book Geurts discusses several ways of engaging and solving a problem. For solving complex problems Geurts suggests - when translated - the following *empirical cycle*: [GEU99]

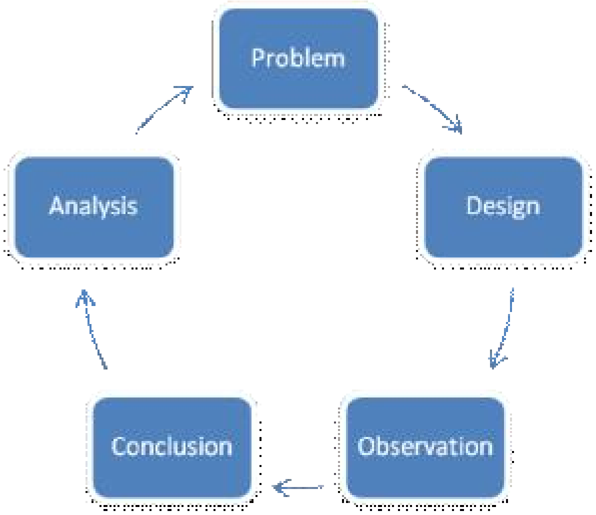


Figure 10: Empirical cycle for complex problems

Notes empirical cycle

The empirical cycle starts of with a *problem*, which leads to a *temporary answer or theory* which is complemented and verified through observations, followed by *analysis* and finally a *conclusion*. This series can be followed by a new problem to form a cycle. The variation on this cycle used in this research project is the interpretation of a temporary answer in the form of a design, not a hypothesis as would have been a more literal interpretation.

It is not mentioned in the book but it will also be presumed that the cycle can be iterative, in which the new problem is only an adjusted version of the starting problem and need not necessarily be a new problem. In this way large problems can, for example, be answered in several steps or divided into several parts.

Block 1: Problem

Geurts concentrates on the *problem*, along with everything of influence on solving it. A research proposal -in this case the project plan- should generate a model to solve the problem and should therefore -according to Geurts- consist of three main elements: [GEU99]

1. Main research question

This question -or in this project; questions- set the domain (scope) of the project, which will be narrowed down even further in following steps. The classification of the different problems the questions address, give an idea of the complexity of the problem and the amount of research that can be expected to have to be done. It also gives a greater verifiability of the results.

2. Specific elements of a problem definition[14]

The second element starts off with the *goals and relevance of the research*. Next is a *theoretical exploration*. This exploration will carry on through the entire research project.

The *choice of the subject(s) of research* will follow from this theoretical background as well as from the performed brainstorm, with input from colleagues and the supervisors.

The *key variables* are the object variables that need to be explored, described, explained, predicted or even changed.

3. Specific elements of the research strategy

The third and last element starts of with *data collection methods*. The method most used is literature research, supported by empirical verification and testing. For some questions case studies are more relevant, for others theoretical models are more interesting. This depends therefore on the question that needs to be answered. In the end the social engineering risk management model needs to be tested. For this a population of organizations is chosen. The tests are performed on location if possible and otherwise at the Atos Origin office campus in Utrecht.

The *analysis plan* should consist of thoughts on the way the collected information should be organized to generate the desired outcome; that is to answer the (main) research questions and with that solve the problem.

The *time, activity and budget planning* are not mandatory. According to Hedrick et al, the resource planning should account for; the *data collected*, so what the sources of information are and how this information can be obtained. [HED93] The *time* necessary for the entire project can be recorded in a project plan and the time per activity in an activity plan. The activities are divided in phases of the project and ordered in each phase by the main research question they support. The last two factors that need to be accounted for according to Hedrick are less relevant to this research. The first is *personnel,* so how many and which researchers need to be available for each activity. This is very simple; the graduate is the only researcher and information is

[14] Geurts uses several kinds of problem definitions. It should not be confused with the problem definition mentioned in the project plan. See section Swanborn.

obtained from other researchers through literature study or interviews, of which the last is very time consuming and only performed if the interviewee has a special expertise which is not available in literature. Only for the testing of the model more interviews are necessary. And finally the last is *money*. The budget is minimal. The highest costs are occurred by the use of office equipment and stationary. This will therefore not be noted any further.

Block 2: Preliminary design

The preliminary design focuses on the generation of a temporary answer to the research problem. During this research the temporary answer has been interpreted as the design of countermeasures and an assessment tool. This design is based on thorough analysis of the information gained by theoretical research as well as case studies on the subject.

Block 3: Observation

The observation is performed during the verification of the preliminary findings and design. This is the empirical research that needs to be performed and is performed in the form of interviews.

Block 4: Analysis

In this second analysis the observations gathered by the empirical research are analyzed. The observations can have different forms, for example comments on the preliminary design or practical experience with social engineering or related subjects. This analysis is used foremost to test the usability of the designed tool, but can also give another perspective on the theoretical research performed before. If necessary the design is changed to generate better results or recommendations will be given to make the development of a full-scale audit easier and generate a better view on the impact of social engineering on specific organizations.

Block 5: Conclusion

And finally in the fifth and last block of the Empirical cycle the conclusions are drawn on both the theoretical as well as empirical research and final recommendations are given for further use of this research and its results. In this block also all research is summarized and recorded in this thesis.

PRINCE2

Next to the framework, some insights were taken from the structured project management method Project IN Controlled Environments (PRINCE2). It focuses heavily on control and states that it is necessary to have a clear approach in place before starting a project, this to organize the project in a logical and controlled way. It was developed by the Office of Government Commerce in the UK as a standard for solving IT project management. The method divides the project into manageable stages which makes it easy to control and monitor the progress. PRINCE2 is product-based so it focuses on the deliverables and not just on the planning. [KEY06] For this small project it is a too heavy and formal method, but some insights have added value over the approaches stated by Geurts and Swanborn.

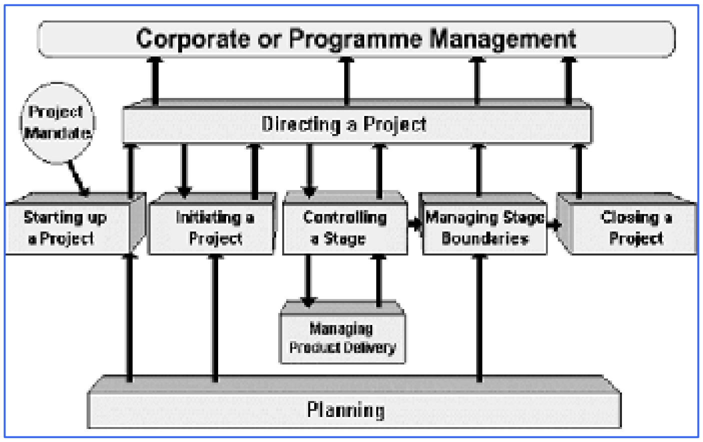


Figure 11: PRINCE2 model

The *start of the project* is in the form of introductory meetings with the supervisors and the obtainment of a project mandate. [KEY06]

This is followed by the *initiation of the project*. The project plan can be seen as a *project initiation document* as it is called in PRINCE2. In this document several things are recorded in the project base and the subsequent steps are described like the steps in the approach of Geurts.

In the middle blocks *managing product delivery* and *controlling a stage* deliverables are generated and the planning should be followed strictly. Discipline is very important in these blocks because there is not a project board looking over your shoulder at all times.

The *managing of stage boundaries* is very important because of its influence on earlier stages. The boundaries and therefore scope of the project, set in the project plan needs to be kept in mind at all times, and if necessary adjusted along the project.

Finally the project ends with the *closing of the project* by producing an end product that meets the wishes of the ‘client’ and own whishes as well if possible. The end products in this research project are the thesis, a graduation presentation and discussion on the research.

PRINCE2 in this research

Two sections of the project initiation document deserve special attention and were added to the project plan: *project assurance* and *controlling change*. [KEY06]

The project board or a project assurance team should normally check the project balance between costs and benefits (*business assurance*), if user requirements are being met (*user assurance*), and that the solution is suitable (*specialist or technical assurance*). During this project the supervisors have performed these checks along the way, by reviewing project updates given and giving feedback during meetings. The costs and benefits are not applicable because of minimal costs. The supervisors therefore focused on the requirements and the suitability of the solution. To maximize the quality of the projects outcome PRINCE2 also manages risks by summarizing the possible risks and alternatives to divert these risks. A *risk assessment* is given next. Another condition to maximize quality is to *test* *or review the work*. Testing of the social engineering risk management model will be done at several organizations. The reviewing will be done by the supervisors. Finally PRINCE2 has a function to prevent straying too far in the wrong direction by *registering changes* which will be used during the writing of the project plan and thesis.

Empirical cycle versus PRINCE2

Now the link between the Empirical cycle and PRINCE2 -which is drawn graphically in the following figure-, will be discussed briefly.

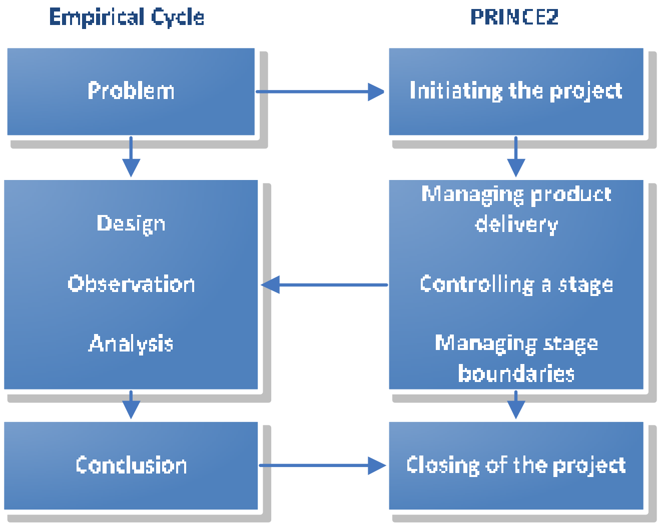


Figure 12: Empirical cycle versus PRINCE2

Both the problem in the empirical cycle and initiating the project in PRINCE2 focus on the problem definition and everything related to it, and generate a project initiation document or project plan (in PRINCE2). In the next three stages the empirical cycle focuses on the practical research and PRINCE2 focuses more on the management to support this research. In the final stage the conclusions are drawn in the empirical cycle and the project is finalized in the PRINCE2 method, which leads to the final thesis. In short the *research* is performed according to the empirical cycle and the *management of the project* and *recording of the findings* is done according to PRINCE2.

Swanborn

The research of Swanborn is discussed elaborately in the book of Geurts. The research and main research questions in the project plan are both classified according to Swanborn into descriptive - also referred to as inventory questions -, explanatory, predictive, remedy and design questions. [SWA90] These are ordered according to their complexity and therefore the amount of work that needs to be done to answer them. The classification gives an idea on the way the answers can be found.

Notes problem and problem definition

Some notes on the problem and problem definition are in order to avoid confusion. Swanborn uses the following definition of a problem definition, again translated: [SWA90]

> *The problem definition is the most complete, timely and*
> *briefly formulated question the researcher can possibly answer.*

In his book Geurts uses a more simple interpretation of this definition, but now for the definition of the main research question. During this research project again a variation on this definition will be used for the main research question:

> *The main research question is the operational formulation of the question which the researcher has to answer.*

Geurts uses the word specific which has been exchanged with operational because the research project is iterative and the specific formulation may change during the project. An operational and usable formulation is therefore more important then a specific formulation.

The description used for a problem definition is simply defined as follows:

> *The problem which needs to be solved by performing the research project.*

Notes main research questions

The first research question focuses on the *risks* associated with social engineering and the *attacks* that can be used in theory and are used in practice. This is a description problem; generating a description of *what* social engineering is and a list what it entails. The second research question is a *remedy question* to solve a therapy problem. This focuses on generating a list of *which* known means (controls/measures) there are, to change a specific (unwanted) state -in this case the vulnerability to social engineering- into another (wanted) state -lowered vulnerability. The last question focuses on *how* an (universal) social engineering risk management model can be designed, a design problem and is therefore a *design question*.

The main research questions together form an *accumulation of knowledge*. [GEU99] This means they all address a different kind of problem and each following question needs input from the previous questions. This takes place in an iterative fashion because new insights will be gained throughout the entire project. During this process it will therefore be cyclical instead of serial as can be seen in the following figure.

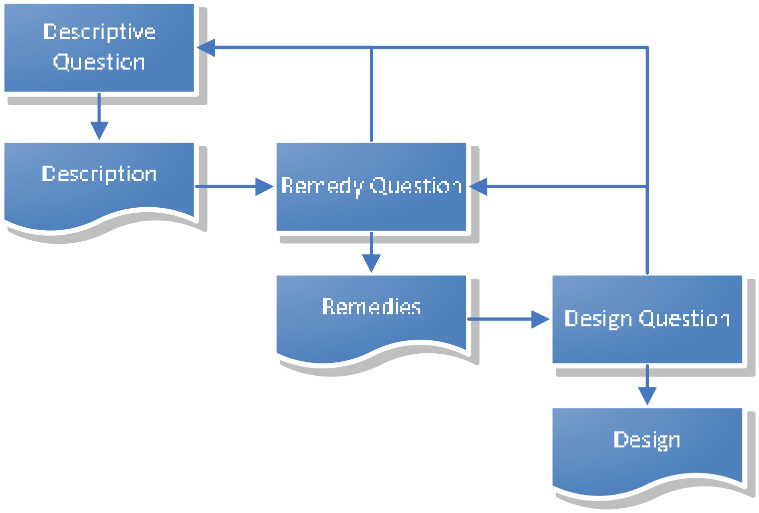


Figure 13: Accumulation of knowledge through main questions

Notes on the research questions

The research questions are ordered according to the main research questions and are classified according to the classification of Swanborn. [SWA90] This gives an indication on the way the collected information can be organized to answer the (main) research questions and with this the overall problem. This is discussed more elaborately in the related project plan.

Project risk model

Du Croix uses a classification of risks in the project plan for his graduation. [DUC04]

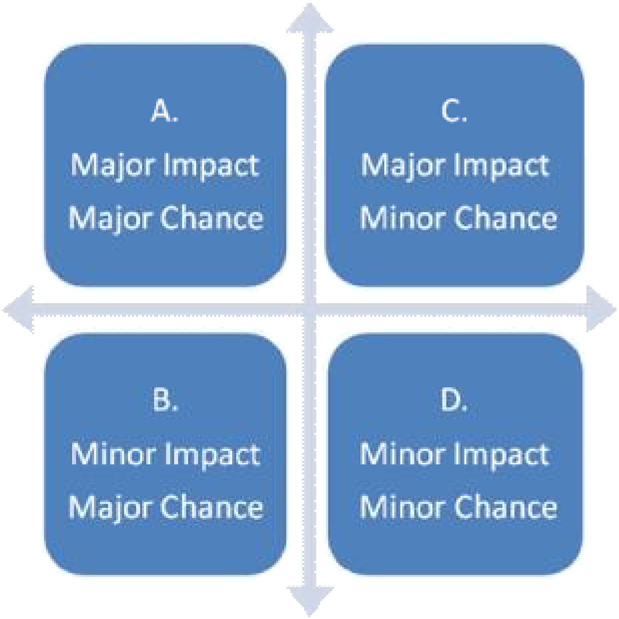


Figure 14: Impact versus Chance matrix

For risks in field A corrective actions are necessary to decrease the chance and impact, for risks in field B impact avoiding actions need to be taken, for risks in field C chance avoiding actions need to be taken and for risks in field D no actions are needed. The more specific risks are discussed in the project plan.

Appendix B: Notes Social engineering attacks

In this appendix an elaboration will be given on the different social engineering tactics and psychological principles listed in chapter 4. Notes will be discussed per phase and information that can aid the social engineer in the tactic –*input information*- will be given next to the organizational information which could be obtained through employing the tactic –*output information*.

Phase 1: Preparation

During this phase information and attributes are gathered to be used to prepare and plan the following phases.

Preparation social engineering tactics

The tactics to gather information and attributes are ordered here from physical to virtual:

1. Physical reconnaissance

During a *physical reconnaissance* the social engineer will study the organization by observation. [JAN05] Using tactics as *shoulder surfing* -which means looking over someone's shoulder- and *eavesdropping* -which means listening to conversation at locations where personnel gathers or public venues- and finally even *tailing* –physically following a person- is performed, all with the intent to store useful information and routines for later use. [ALL06] [BEA04] [JON03] [RED05]

Input Information	Output information
-	§ Employee names § Employee function § New employees § Lingo

2. People spotting

Closely linked to physical reconnaissance is the tactic *people spotting,* which is the hanging around a certain location for some time to spot targets for tailing and/or social engineering. [BEA04]

Input Information	Output information
-	§ Employee names § Employee function § New employees § Lingo § Organizational policy and processes

3. Dumpster diving

Dumpster diving or trashing means that the attacker goes through the trash of an organization looking for potentially useful information that should have been discarded more securely or attributes that can be used in other phases like stationary. [ALL06] [BEA04] [GRA01] [MIC06] An important aspect of this tactic is that it does not pose any threat to the social engineer in itself because it is not illegal in many countries. [ART01]

Input Information	Output information
-	§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § IT infrastructure § Organizational logos

4. Forensic analysis

Linked to dumpster diving *forensic analysis* is performed on discarded computer equipment like hard drives, memory sticks and removable media to gather information that should have been removed permanently. [ALL06]

Input Information	Output information
-	§ Employee names § Employee functions § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § IT infrastructure § Organizational logos

5. Phreaking

Phreaking means breaking into a telephone system (PBX) to use this in the following phases by for example changing the phone number exposed with caller ID or rerouting calls to the social engineers (cell) phone. [BEA04]

Input Information	Output information
§ Internal phone numbers	-

6. Phishing

Phishing is the fishing for information and passwords by ‘masquerading as a trustworthy person or business in an electronic communication’. [GRA06] [KAN07] [WIK06] In the past it was performed by phone, explaining the first two letters. In the current computer age it can for example have the form of an e-mail or pop-up directing to a fake website looking exactly like a trusted parties' in which the target needs to sign up with his or her password. [ALL06] [GRA06] [GRG02] [MIC06] [MIT02]

Input Information	Output information
§ E-mail addresses	§ Organizational structure
§ Internal phone numbers	§ Employee names
	§ Employee functions
	§ Calendars
	§ Internal phone numbers
	§ E-mail addresses
	§ Organizational policy and processes
	§ Lingo
	§ User names
	§ Passwords

7. Mail-outs

There are several kinds of *mail-outs*, for example in the form of surveys. These are used to gather corporate and personal information and fall under phishing. Participation in these surveys is increased by offering enticements like prizes, in which case they are contests. [ALL06] But mail-outs can also be used to set people up for reverse social engineering or to send malicious software as will be discussed further on. [RED05]

Input Information	Output information
§ E-mail addresses	§ Organizational structure
	§ Employee names
	§ Employee functions
	§ Calendars
	§ Internal phone numbers
	§ E-mail addresses
	§ Organizational policy and processes
	§ Lingo
	§ User names
	§ Passwords

8. Web search

Jones indicates several *web based tactics* that can be used to gather information. [JON03] Search engines, newsgroups, job sites and corporate websites all offer valuable corporate and personal information. [DOL04] [GRG02] [JON03] [KIE06] [MIC06] [RED05] Most organizations do not even know where and how secure their information is stored by other parties and therefore how easily attainable for the social engineer.

Input Information	Output information
-	§ Organizational structure
	§ Employee names
	§ Employee functions

	§ E-mail addresses § Organizational policy and processes § Lingo

9. Profiling

The preparation also includes the transformation of the gathered information to be useful in the following phases and planning of the following steps. One tactic linked to this aggregated information is *profiling*, which is the creation of a profile on a chosen target to exploit or to impersonate using for example lingo and routines. [JAN05] [ALL06] This profile will be used to reveal weaknesses or create scripts to manipulate the different targets using the gathered knowledge, creating authenticity by knowledge of business processes and internal language. [GRA01] [DOL04]

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo	§ Target profile § Attack plan § Attack scripts

Next to the input information gathered from the organization, sources of technical information can be used to plan the execution phase.

Phase 2: Manipulation

Social engineers use several tactics to manipulate their targets. [DUD06] [MIC06] The basic psychological principles underlying these tactics are linked to human nature and situations in which a target is more vulnerable. These will be discussed next, followed by the actual tactics used by social engineers to manipulate the target.

Psychological principles

In current literature a lot of attention is given to the basic psychological principles used by the social engineer to extract the needed information. [JON03] Gragg defines 'psychological principles that exhibit some kind of power to influence or persuade people' called *triggers*: Strong affect, overloading, reciprocation, deceptive relationships, diffusion of responsibility and moral duty, authority, and integrity and consistency. [GRG02]

Strong affect

This trigger focuses on a heightened emotional state during which a target is less likely to stop and think to evaluate the arguments a social engineer poses and come up with a counterargument. This gives the social engineer the means to persuade a target with only weak arguments to do something that they reasonably would not do normally, by creating a *mental shortcut* –'a leap in logical thought' [RED05]. The emotions the social engineer will trigger include fear, excitement and panic.

These heightened emotional states can be created by a feeling of *scarcity*. When the target believes the object is in short supply, only available for a short period or others are competing for it, he or she will be more willing to comply with the wishes of the social engineer. [MIT02] A similar reasoning can be used for the emotional state created when the target is confronted with *urgency*, in both cases the target needs to make a decision quickly and does not want to be held responsible for the consequences. [RED05]

Another example is *counterfactual thinking*, which is the strong influence on a target's reasonable thinking by the anticipation of the possibility of winning a big prize. [GRG02] The anticipation is so great that the target forgets that the chance of winning is still remote and risks information or access for this remote change. Surprise can therefore be a strong means of persuading a target because the target is not thinking straight at that moment. Emotions caused by this surprise – positive and negative – will be used by the social engineer. [GRG02]

Overloading

This trigger focuses on overloading a target's senses by a large amount of information. This overload will influence the logical functioning of the target and makes the target passive, also known as 'dummy mode'. [BEA04] The target will need to create mental shortcuts to try and keep up with the social engineer. The social engineer will use this to slip an unreasonable request in between normal requests and the target will not notice it anymore.

Another means of overloading is arguing from an unexpected perspective. The target will not be able to reason in the small amount of time available and will again not be able to evaluate arguments correct.

Reciprocation

This trigger focuses on the return of a favor or the promise of something valuable. [RED05] In social interactions it is perceived normal to return a favor if someone does something for us or promises something, even if the original favor was not asked for or the favor requested in return is much more valuable then the original given. [MIT02] It is in human nature to be trusting and a target will therefore use a mental shortcut to reason that a helpful person is to be trusted. [MIT02]

Another form of reciprocation is to give in during a disagreement after the other party has given in. A social engineer will ask for several things and give in on one to get the other(s). [CIA00]

People see this system of favors as a means to get up in the organization, to lead a successful career and do not see the harm they can cause. [GRG02] [ALL06]

Deceptive relationships

This trigger focuses on building a relationship to exploit this trust to the fullest. A relationship can be build by casual contact without any requests or by sharing information with the target -in which case it uses the reciprocation principle once again- after which the target is happy to give away information to the social engineer without even asking. [ALL06] [MIC06]

Another way of building a relationship is by finding or creating a personal connection, using this to convince the target that he or she and the social engineer are alike and have the same interests therefore generating a false feeling of trust. [JON03] [ALL06] [CIA00]

Being friendly and likeable can therefore be very useful in obtaining information. [CIA00]The target wants to believe the social engineer when impersonating a trustworthy person and will respond in a friendly helpful way. Social engineers therefore only need to be believable to use this principle. [GRA01] He or she will try not to ask suspicious questions but instead use a series of conversations to gather small peaces of information.

In larger organizations it is easier to create a relationship based on fiction and establish trust, in smaller organizations the chance is greater a target will know the person the social engineer is impersonating or referring to –*name dropping*. [MIT02][JON03] [DOL04]

Diffusion of responsibility and moral duty

The trigger diffusion of responsibility focuses on creating a feeling with the target that they will not be held (solely) responsible for an action they perform which alleviates the stress on the target. [ALL06] [GRA01] [STE02] This can be enhanced by *moral duty*, because the target wants to help the organization or person on the other end and does not want to feel guilt. [ALL06] [RED05]

Authority

This trigger focuses on the feeling of authority linked to specific functions in the organization or community. [JON03] [MIT02] 'People are conditioned to respond to authority'. The target will go to far lengths to please someone in authority. In many organizations it is not accepted to challenge authority, which makes it hard to verify the true authority of a person. [GRG02]

Integrity and consistency

The trigger integrity focuses on the tendency to follow through on commitments made, even if they seem unwise. [MIT02] Targets do not wish to be seen as untrustworthy or be reprimanded for their act. The target will therefore wish to fulfill his or her promises or even the promises the target believes are made by coworkers. [GRG02] This tendency to use the (presumed) actions of others as validation appeals to the trigger *consistency* or conformity also known as social validation. [MIT02] [GRG02] [GRA01]

In summary all these psychological principles focus on the creation of a feeling of trust or a situation in which the target will not be likely to challenge the request of the social engineer.

Manipulation social engineering tactics

Now the actual attack tactics based on the psychological principles will be discussed:

Impersonation in general

Impersonation means acting out a script of a role or specific individual, also known as play-acting. Impersonation moves some of the risk from the social engineer because the true identity is still unknown when exposed. [RED05] It can be performed *virtually* –using a medium- or *physically* –in person. [BEA04] [KAN07] Most common roles that are used include: [GRA01]

§ An authority

By using *clout* -the authority of a specific function within the organization like a manager or someone calling on behalf of a manager- a target can be influenced into providing information or access. [ALL06] [DOL04] Most employees want to impress the boss, so they will bend over backwards to provide required information to anyone in power. [GRA01] [ALL06] The social engineer will use this status of authority to *intimidate* the target, for example by threatening with consequences if the target does not comply with the social engineer's requests. [RED05]

§ A colleague

By impersonating a colleague trust can be gained and information and access obtained through unsuspicious targets. [JAN05]

§ Someone needing help

By pretending to be a helpless user -like an *intern* or *new employee*- the social engineer can convince the target –for example *helpdesk personnel*– into providing information or access. [ALL06] [MIT02] [RED05]

§ Someone offering help[15]

By pretending to be (technical) support personnel or an employee of a trusted third party -like the software provider- that needs the information the target possesses to guarantee support, the social engineer can obtain vital information like usernames and passwords. [ALL06] [MIT02] [JON03] This is closely linked to *reverse social engineering*.

10.Physical impersonation

This tactic is used when the social engineer needs to enter the organization or any other location to achieve his or her goal. [MIC06] During the usage of this tactic the social engineer will need to interact with targets in person. The penalty of even a small mistake can be much larger then in virtual impersonation. The risk for a social engineer when applying this tactic is therefore great. Only skilled social engineers will apply this tactic when great benefits can be obtained.

[15] Also see 'Reverse social engineering'.

Because of the consequences of the social engineer being ‘burned’ (exposed) when colleagues cannot authenticate the identity, the social engineer will choose a role which will be less easily challenged –an authority- or someone less suspicious and more difficult to authenticate –an intern, new employee or third party- over the role of a normal colleague. [BEA04] [RED05]

11.Virtual impersonation

When the social engineer does not wish to run the risks physical access entail he or she will keep a save distance by using a medium for the interaction with the target. A medium can be a phone, fax, website[16], e-mail or plain mail and can be just as effective as personal interaction in gaining information. [MIC06]

With physical impersonation the preparation may use more and more specific information and physical attributes may be used during the attack, but the basic information input and output are the same for both types of impersonation.

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § Target profile § Attack plan § Attack scripts	-

12.Reverse social engineering

The basic idea of reverse social engineering is that the target comes to the social engineer instead of the other way around –like in impersonating someone offering help. [MIC06] The social engineer will cause a situation in which the target needs the help of the social engineer. [KAN07] This can for example be accomplished by creating a problem on the targets computer or network or even simply by making the target believe this. The social engineer will offer his or her services to solve the problem and with this gain trust with the target. [DOL04] Typical reverse social engineering consists of three phases: [ALL06] [GRA01]

[16] Also see ‘Phishing'.

- Sabotage

  This means the social engineer creates a problem on the computer or network of the target or gives it this appearance. After which the target will need help.

- Marketing

  This means the social engineer needs to get the target to ask for his or her help by for example advertising with business cards[17] or a support address in the error message.

- Support

  This means that the social engineer will give the target the impression he or she is being helped. [MIC06] At the time of this assistance the social engineer can obtain information or access, or could create trust which could later be used.

Reverse social engineering requires a lot of preparation and research to be a success. [MIT02] [ALL06] [GRA01] [JON03] [GRG02]

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § Target profile § Attack plan § Attack scripts	-

Phase 3: Exploitation

The goals of a social engineer are linked to the motives discussed in chapter 3: People hacking and can therefore differ greatly. If the final goal is to get the target to 'reveal information or act in a manner that results in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data', this can be reached in this phase.

Exploitation social engineering tactics

Although the manipulation already occurs in the previous phase the products of the exploitation of the influenced targets will lead to the information or data the social engineer is after. The social

[17] Also see 'Item dropping'.

engineering tactics applied in this phase are mostly focused on *physical access* because the virtual impersonation and reverse social engineering cover all attacks using a medium.

10.Physical impersonation

This tactic forms the bases for the physical access discussed further on. By itself it does not yield any information and uses the information as already stated in the previous phase.

Input Information	Output information
§ Organizational structure	-
§ Employee names	
§ Employee functions	
§ New employees	
§ Calendars	
§ Internal phone numbers	
§ E-mail addresses	
§ Organizational policy and processes	
§ Lingo	
§ Target profile	
§ Attack plan	
§ Attack scripts	

11.Virtual impersonation

Through virtual impersonation the social engineer can -in theory- reach any goal within the definition: information or unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data. The social engineer can therefore obtain any information available on the organizational infrastructure. [BEA04]

Input Information	Output information
§ Organizational structure	§ All information
§ Employee names	
§ Employee functions	
§ New employees	
§ Calendars	
§ Internal phone numbers	
§ E-mail addresses	
§ Organizational policy and processes	
§ Lingo	
§ Target profile	
§ Attack plan	
§ Attack scripts	

12.Reverse social engineering

With reverse social engineering the same goals can be reached as with the virtual impersonation, all information can be obtained.

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § Target profile § Attack plan § Attack scripts	§ All information

13.Tailgating

Tailgating is one of several ways of gaining access to an office or restricted (physical) area. It is simply following an employee or delivery staff whit legitimate access into an area without proper authorization or providing verification. [JON03] The social engineer will for example just wait for someone to open a secure door and step in before it closes, without anyone getting suspicious. [MIC06] The access by itself therefore does not need any information, but the social engineer will need a fallback plan to cover when questions are asked, in the form of *physical impersonation*. In this case it can be very basic, but the information necessary for physical information can be very helpful. Information is not yet gathered with this access, but will be gained by *office and desk snooping*.

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § Target profile § Attack plan § Attack scripts	-

14.Piggybacking

At large organizations most employees do not know every coworker and will hold a door for someone. [DOL04] This tactic uses the politeness of the people to gain access and needs contact with the employee or other person with legitimate access. [JON03] [RED05]In contrast to tailgating this contact with other people will force the social engineer to impersonate someone with legitimate access. The same information as with *physical impersonation* will therefore be necessary. And again no output information is gained at this time.

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § Target profile § Attack plan § Attack scripts	-

15.Office snooping/Desk sniffing

Once on site by *tailgating*, *piggybacking* or any other way the social engineer can easily attain any information that can help plan and execute following phases or attacks. [GRG02] [Lively] [ORG04I] The social engineer will just walk around the office and snoop on desks and in cabinets of employees who have stepped away. [DOL04] During office hours the social engineer will be very cautious and will need to work fast. But when the social engineer obtains access outside working hours -by for example posing as a cleaner- he or she can take a lot more time and will less likely be detected snooping through papers and computers.

Input Information	Output information
-	§ All information

16.Item dropping

When the social engineer is inside the organization the social engineer can leave something behind. This could for example be a CD or message on the internal mail with malicious software. [RED05] But also a helpdesk number for a *reverse social engineering* attack. [MIT02] This does may use some basic information on the target or could be totally random. By itself it does not yield any information.

Input Information	Output information
§ Employee names § Employee functions § New employees § E-mail addresses § Organizational policy and processes § Lingo § Target profile	-

17.Data leakage

Data leakage is a very specific tactic focused on the direct or constant leaking of information from a technical system. [PRO06] This can be done by hardware installed by the social engineer during physical access. [MIT02] Or by software which could be installed during physical access, be left through item dropping or even sent by mail, in which case it is a form of *malicious software*.

Input Information	Output information
§ Target profile	§ All information

18.Direct approach

A social engineer can use the direct approach and ask the target directly to give the information or access the social engineer is after. [ALL06] [DOL04] [DUD06] [JON03] [MIT02] It is the most straightforward tactic, but also most probable to be noticed, making the target suspicious and therefore useless for further manipulation. [ALL06] [STE02] More often the social engineer will use a series of calls to multiple individuals to gather the information and/or access needed to cause damage. [DOL04] When the target complies with the request without posing questions the social engineer will not need any information next to the contact information of the targeted employee.

Input Information	Output information
§ Internal phone numbers § E-mail addresses	§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes

Phase 4: Execution

Although a successful social engineering attack does not require a great deal of technical knowledge, using technology in conjunction with social engineering principles can be very effective. [DOL04] [MIT02]

Execution social engineering tactics

Attacks and countermeasures in the execution phase mostly have a technical nature and are more in the field of hacking then social engineering. [DOL04] Therefore only two tactics in the execution phase will be discussed shortly in the context social engineering.

19.Identity theft [MIT02]

The use of information acquired in the previous phases can be used to impersonate an employee or other individual in real life or online. In general passwords and credit card information is used to enter electronic pay sites or access and empty bank accounts. [GRA06]

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Calendars § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § Target profile § Attack plan § Attack scripts	-

20. Malicious software

Malicious software can spread in several ways, for example attached to an e-mail or on items that can be left around the office. A more specific form is a chain mail for example warning for a virus outbreak. Such a mail can cause a snowball effect because everyone forwards it. [ALL06] It can also have several shapes; a virus, a Trojan horse, key logger[18], etc. [ALL06] [RED05] One thing all malicious software has in common; it will harm the person installing it and is created for this purpose.

Input Information	Output information
§ Organizational structure § Employee names § Employee functions § New employees § Internal phone numbers § E-mail addresses § Organizational policy and processes § Lingo § Target profile § Attack plan § Attack scripts	-

[18] A key logger is software that sends all keystrokes of the target to the social engineer, including login codes and passwords.

Summary

In summary most information is gathered in the preparation phase. This is used to manipulate the target -using a number of psychological principles- in the manipulation phase. Which in turn leads to reaching the goal by exploitation of these people and when necessary executing a final attack.

Appendix C: Notes Empirical research

In this appendix the leading questionnaire in original Dutch and a translation in English are given, next to the findings generated from comparing notes from the different interviews.

Dutch questionnaire

Uitleg afstuderen.

Bedoeling van dit interview.

Alle informatie wordt strikt vertrouwelijk behandeld.

Gehanteerde definitie van Social engineering:

Social engineering is de succesvolle of onsuccesvolle poging een persoon of personen te beïnvloeden informatie te openbaren of zich zo te gedragen dat dit resulteert in de ongeautoriseerde toegang, ongeautoriseerd gebruik of vrijgave van een informatiesysteem, een netwerk of data.

1. Bent u het hiermee eens? Hoe kijkt u er tegenaan?

Uitleg analysemodel.

Assessment

Stap 1: Organisatie beschrijving

2. Kunt u een beschrijving geven van de organisatie en de verschillende afdelingen daarbinnen?
3. Wat wordt er gedaan binnen de organisatie? Welke processen vinden er plaats?
4. Wie zitten er op de verschillende afdelingen? Wat voor (ondersteunende) functies?
5. Wie heeft verder nog toegang tot de organisatie en haar informatie?
6. Welke informatie is toegankelijk vanaf de afdeling en/of wordt daar verwerkt?
7. Welke informatie en data zijn aanwezig of toegankelijk vanaf de verschillende afdelingen?
8. Hoe wordt deze informatie en data opgeslagen op de verschillende afdelingen?
9. Welke informatiesystemen en netwerken zijn aanwezig of toegankelijk vanaf de verschillende afdelingen?
10. Welke communicatiemiddelen worden gebruikt op de verschillende afdelingen?
11. Hoe gaat informatie door de organisatie? Is hier een structuur voor?

Stap 2: Identificatie bedreigingen

12. Welke bedreigingen ziet u vanuit social engineering m.b.t. de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen uw organisatie?
13. Welke motieven zou een social engineer kunnen hebben om de organisatie aan te vallen?

14. Op welke informatie zou de social engineer uit zijn? Welke zou hij of zij gebruiken in zijn of haar aanvallen?

15. Welke bedreigingen ziet u vanuit uw eigen personeel en externe partijen binnen de organisatiegrens?

16. Welke bedreigingen ziet u vanuit hacking?

Stap 3: Identificatie kwetsbaarheden

17. Is er een kwetsbaarheidanalyse uitgevoerd?

18. Wat waren de uitkomsten hiervan m.b.t. social engineering?

19. Kunt u nog andere kwetsbaarheden aangeven binnen uw organisatie?

20. Worden er incidentrapporten opgemaakt?

21. Zijn er recent nog incidenten geweest m.b.t. social engineering?

Stap 4: Analyse controls

22. Hoe wordt de informatie, data, informatiesystemen en netwerken beschermd?

23. Wat is het doel van de bescherming?

24. Wat zegt het beleid hierover?

25. Welke controls zijn aanwezig? Fysieke, organisatorische, software en hardware bescherming.

26. Hoe vindt het in de praktijk plaats?

27. Is dit naar uw mening voldoende om het risico van social engineering af te dekken?

28. Zijn er nog nieuwe controls gepland?

29. Is bekend welke informatie reeds buiten de afdeling bekend is, waar en hoe er daar mee omgegaan wordt?

Stap 5: Analyse waarschijnlijkheid

30. Kunt u op basis van uw antwoorden op voorgaande vragen de waarschijnlijkheid van een (succesvolle) aanval aangeven? Laag, middel, hoog?

Stap 6: Analyse impact

31. Wat zijn de mogelijke gevolgen voor de organisatie als informatie openbaard wordt aan ongeautoriseerde personen of niet (meer) betrouwbaar of aanwezig is? Laag, middel, hoog?

32. Heeft uw organisatie een classificatie gemaakt van de informatie, data, informatiesystemen en netwerken aanwezig en toegankelijk vanaf de verschillende afdelingen?

33. Hoe kritiek/waardevol zijn de verschillende afdelingen en haar informatie, data, informatiesystemen, netwerken voor de organisatie? Welke informatie is waardevol?

34. Hoe gevoelig zijn de informatie, data, informatiesystemen en netwerken m.b.t. de vertrouwelijkheid, integriteit en beschikbaarheid? Welke informatie is gevoelig?

Stap 7: Vaststelling risico

35. Welke risico's denkt u nog te lopen op basis van de waarschijnlijkheid van een social engineering aanval, de gevolgen ervan en de controls die u hebt genomen?

Stap 8: Aanbevelingen

36. Welke controls denkt u nog te moeten implementeren om tot een acceptabel risiconiveau te komen?

Stap 9: Documentatie

Niet relevant op dit moment.

Stappenplan

37. Vond u het doorlopen van de vragen nuttig?

38. Vond u het doorlopen van de vragen gebruiksvriendelijk?

Dank u voor dit interview!

English translation of questionnaire

Explanation graduation project.

Intention of the interview.

All information will be handled strictly confidential.

Definition of social engineering used in thesis:

> *Social engineering consists of the successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data.*

1. Do you agree with this definition? How do you see social engineering?

Explanation analysis model.

Assessment

Step 1: Organizational description

2. Can you describe the organization and its different divisions?

3. What does the organization do? Which processes are performed?

4. Which functions are present in the different divisions?

5. Who else has access to the organization and its information?

6. Which information is available and/or processed in the different divisions?

7. Which information and data is present or accessible from the different divisions?

8. How is this information and data stored in the different divisions?

9. Which information systems and networks are present or accessible from the different divisions?

10. Which means of communication are used in the different divisions?

11. How does information flow through the organization? Is there a specific structure for this?

Step 2: Threat identification

12. Which threats from social engineering to the confidentiality, integrity and availability of information can you identify within your organization?

13. Which motives would a social engineer have to attack the organization?

14. Which information could be targeted within the organization? Which information would the social engineer use in his or her attack?

15. Which threats from your organizations own personnel and external parties within the organization can you identify?

16. Which threats from hacking do you see?

Step 3: Vulnerability identification

17. Has a vulnerability assessment been performed in the past?

18. Which findings were there related to social engineering?

19. Can you identify other vulnerabilities within your organization?

20. Are incident reports made?

21. Have there been incidents related to social engineering recently?

Step 4: Control analysis

22. How are the information, data, information systems and networks protected?

23. What is the objective of this protection?

24. What is stated in (security) policy on this?

25. Which mitigating controls are implemented? Physical, organizational, etc.

26. Are these controls followed in practice?

27. Are these controls sufficient to mitigate risk of social engineering in your opinion?

28. Are new control implementations planned in the near future?

29. Is known within the organization which information is already available outside the division, where this is available and how the information is used, stored and secured there?

Step 5: Likelihood determination

30. Based on the previous answers, can you assess the likelihood of a (successful) attack? Low, medium, high?

Step 6: Impact analysis

31. What would the consequences for the organization be of unauthorized release of information or loss of confidentiality or availability? Low, medium, high?

32. Have the information, data, information systems and networks present in or accessible from the different divisions been classified?

33. How critical/valuable for the organization are the division and her information, data, information systems and networks? Which information is valuable?

34. How sensitive are the information, data, information systems and networks related to confidentiality, integrity and availability? Which information is sensitive?

Step 7: Determine risk

35. Which risks do you think are still present, based on the likelihood and possible consequences of a social engineering attack and the implemented controls?

Step 8: Recommendations

36. Which controls -in your opinion- should still be implemented to get to an acceptable risk level?

Step 9: Documentation

Not relevant for this walk through.

Walk through

37. Did you find the walk through of this questionnaire useful?

38. Did you find the walk through of this questionnaire user friendly?

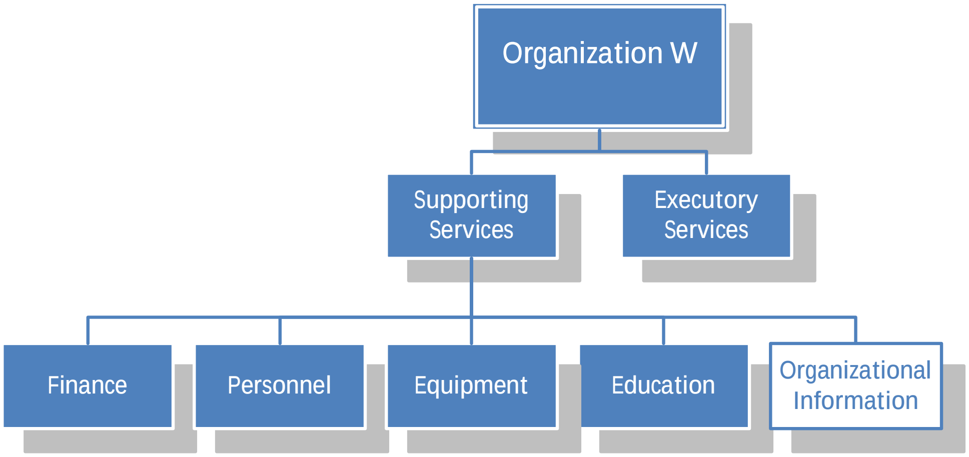
Thank you for your cooperation!

Interview findings

The findings from the interviews have been made anonymous and have only in part been related to the organizations or market. The confidential use of interview findings was a precondition for cooperation of the organizations as the provided information could be used in identifying participating organizations and vulnerabilities within these, which is surely not the intention of this research. Therefore diagrams and organizational descriptions cannot be made any more detailed and less cryptically. The following findings are related to the organizations activities and are structured according to the stages of the questionnaire followed by relevant comments not directly related to the questionnaire.

Example interview report; Regional governmental organization

The second interview was with a regional governmental organization:



The organization is divided in two parts, one executive in which the main activities are performed, the other supporting in which administrative activities are performed. The interview clearly focused on the organizational information division. The interview was held with the Chief Company bureau services, responsible for the organizational information.

Definition social engineering

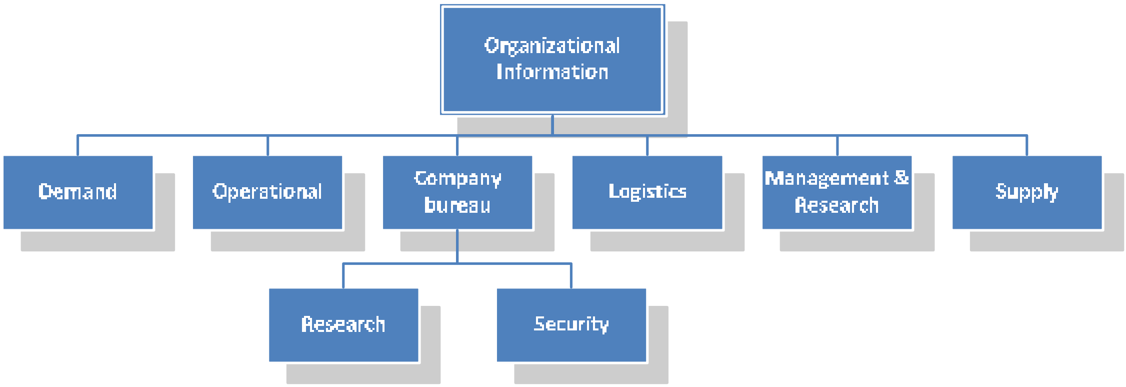
The interviewee was not familiar with the term 'social engineering' but did recognize the description and examples. During the interview the stated definition was used as reference.

Assessment

The walk through of the model gave several insights, per step these where:

Step 1: Organizational description

A first introduction was already given. The diagram given above is the organization as it is deployed per district. As the interview focused on the 'organizational information' division the organizational description also follows this.



The workplace and workstations are not related to the functions except for data mining. Access in not restricted to the local environment, however private use is restricted. Internet access is only available when necessary for the role or function an employee performs.

The functions can be divided in three groups; primary, supporting and management. Authorizations are granted on a need to know base and related to functional profiles. More authorizations may be provided on request. Segregation of duties is implemented within and between the functions.

There are also external researchers that have specific authorizations. As well as temporary laborers, consultants, free lancers and interns. According to specific legislation these should all be screened (even cleaners), have signed a non-disclosure agreement and be under supervision of authorized personnel.

Step 2: Threat identification

The organization handles highly sensitive information, which is of great interest to criminal organizations as well as curious social engineers and hackers. No more specific description can be given to the targeted information. But in general all information in the organization is of interest and can be of use to the social engineer.

A short list of threats where identified, detailed threats more specific to the organization have not been listed:

§ Internal reports do not follow a workflow and can be anywhere on the work floor.

§ Not all information is classified and can therefore be handled improperly.

§ Access is logged. However it happens that people log on another’s profile or password.

§ Some external parties need access to the system before they can be screened. However these persons should be under supervision constantly.

§ It is possible to intercept (classified) communications.

- People working at home create a threat.

Step 3: Vulnerability identification

Some vulnerabilities can be derived from the threats:

- It is not known where information is during processing; there is no accountability.
- Classification procedures are not followed.
- The password security policy is not followed.
- The authorization process is not suitable for some activities.
- Some means of communication are not secure, however they are necessary for operations.
- Procedures for media usage are not followed.
- People do not follow the information security procedures outside the office.

Just before the interview this organization was faced with bad media coverage due to leakage of information after careless handling. The organization thereafter performed a specific assessment on the information crossing the organizational boundary, this lead to the implementation of specific controls to counter this vulnerability.

Step 4: Control analysis

Some examples of controls are listed here:

- Policy is implemented to stop information from crossing the organizational boundary. USB ports are for example generally disabled.
- Information that does need to leave the organization on a memory stick or over the internet is secured through encryption.
- There is an awareness project that relates to the awareness of the information you use and training in how to use this so it stays secure.
- Leakage through personal contacts, in general by accident, is traced and measures are taken if necessary.
- There are heavy penalties on deliberate leakage.
- Physical access is restricted through specific measures.
- Penetration tests are performed, focusing on technical hacking through for example WIFI-connections and blackberries. But also social engineering is tested through physical penetration testing and desk sniffing. The findings from this are used to confront people during the awareness trainings.

Step 5: Likelihood determination

There is a fair likelihood a social engineer can gather information from this organization. However, more critical information will be less likely to leak due to the need to know basis on which it is spread through the organization. In contrast, some threats on less critical information are simply accepted. So the likelihood depends on the information and cannot be determined in general.

A detail: hackers have not been able to penetrate the organization in some time (*ed.* or they are so good that they do not leave a trace).

Step 6: Impact analysis

There are two general consequences of a (successful) social engineering attack;

- The image of the organization can be harmed.
- The organizational processes and even people can be harmed.

Step 7: Determine risk

Even though awareness training and penetration tests are implemented there is still some social engineering risk. The organizational process sometimes prevails over the risk of leaking information. However, the risk is still present due to careless personnel.

Step 8: Recommendations

Organizations need to follow a security management process consisting of a policy statement, followed by awareness, in turn followed by audits. In discussion with the interviewee the following controls where identified which where already implemented (in part), but had not come to light earlier;

- Authorization management should be implemented.
- Physical access should be restricted through for example access gates.
- Data should always be classified.
- Physical pieces of information should be kept behind locked doors or in a fault.
- Server rooms should also be locked and hard disks with confidential information should be kept behind locked doors as well.
- Audits should be performed on the adherence to policy and procedures.

A general conclusion was that people see the world around them in which information is stolen, however they do not see they also need to be careful with information they handle. Awareness training needs to remove this misconception and bring them back to reality.

Step 9: Documentation

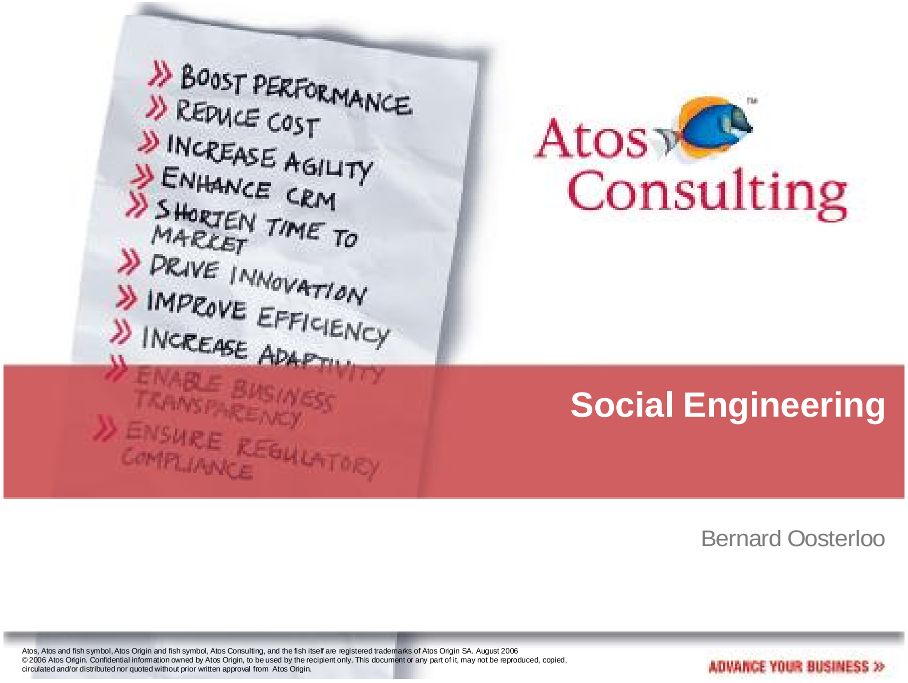
This interview report is the only released documentation.

Walk through

The interviewee did not find the model added much value in this form to their implemented procedures and audits, as it was just ‘yet another model’. If it would be implementable in the current (quality and security) process it would be more useful.

Presentation Information security seminar

In the digital version of this thesis the presentation given at the Information Security Seminar can be viewed by clicking on the first slide below. It should however be noted this is a Dutch presentation.



Social Engineering

Bernard Oosterloo

Summary

The following findings are a composition from all interviews, discussions and organizations and are again structured according to the stages of the questionnaire followed by relevant comments not directly related to the questionnaire:

§ The interview introduction did not give relevant results except interest or disinterest for the project.

§ The interviewee introduction confirmed all participants where indeed responsible for information security, had a good overview of the organization and security therein and could influence the security process in light of their function.

§ All participants were -at some level- familiar with the phenomenon social engineering. However, two interviewees did not relate this to the term 'social engineering', which was unknown to them. After some small explanation all participants confirmed the definition.

§ The model walk through gave several insights, per step:

Step 1: Organizational description

§ All participants gave a clear description of their organization and provided supporting documentation if necessary. They had a clear overview of what was happening in the organization and where the (security) bottlenecks lay.

Step 2: Threat identification

§ After explaining the model of a social engineering attack -as discussed in chapter 4: 'Social engineering attack'- all participants could identify several threats to their information.

§ In the governmental organizations the political motivation is strong next to all others. In the other organizations this is less relevant, but all other motives could create a threat.

§ All organizations had information that could be of value to the social engineer. They also have all information necessary for an attack available and most of this is not seen as relevant in the information security process.

§ Personnel, external parties and hackers are all seen as possible threat sources. But in some cases operational effectiveness prevails over information security, creating vulnerabilities.

Step 3: Vulnerability identification

§ In all organizations vulnerability assessments have been done on their technical systems and physical security. The human is in general only taken in when relevant to the technical systems or physical security. However, this is focused more on internal threats and carelessness of personnel then on the manipulated erosion of information security. The

GOVCERT -being a security specialist and having an exemplary role- also performed a vulnerability assessment as to social engineering.

- After presenting some examples the participants could identify several vulnerabilities which they did not see as related to social engineering. For some of these (incident) responses where already in place through their link with technical systems or physical security.
- One organization was confronted with bad media coverage due to leakage of information and therefore performed a specific assessment on the information crossing the organizational boundary. This lead to the implementation of specific controls to lower this vulnerability.

Step 4: Control analysis

- All organizations have implemented several (information) security controls, physical, organizational and technical. And see the necessity of these controls.
- All the organizations have security policies and procedures. However in four out of five these are not completely adhered to. This can be caused by practical reasons as it lowers operational effectiveness or can be caused by plain ignorance and laziness of the personnel, which in turn can be derived fro the security culture. If the organizations therefore do not monitor the security process actively, policy and procedures do not have effect and a culture of limited security is created.
- One thing the organizations worry about is the leakage of information by their own personnel, just by taking information across the organizational boundary. Therefore awareness on this specific subject is stimulated. However, none of the participants could give a clear estimate on the amount of relevant information on the organization available outside the organization.

Step 5: Likelihood determination

- The answers here are not rosy as most participants needed to admit that their security related to social engineering is not on to par and could be breached. One participant however mentioned that the operational effectiveness was more important then the security of the information at risk at this time. Another said the level could and would be raised when a greater budget was available.

Step 6: Impact analysis

- This differs greatly between the different organizations and systems. Albeit that even when information was classified this left out information relevant to social engineering. This should have been classified.

Step 7: Determine risk

- All participants had to answer that the social engineering risk will never be completely eradicated, surely cost effectively.

Step 8: Recommendations

- The different organizations lead to different recommendations. But most important is the implementation of good policy and procedures, implementing these along with supporting awareness trainings and auditing the compliance to these.

Step 9: Documentation

These have been described in this appendix.

- In general the organizations found a social engineering risk management model to specific to implement completely next to already implemented risk management processes and models. They did however see the potential of such a model if it was in line with the already used processes, models and best practices.

The preliminary design of the social engineering risk management model was updated where necessary according to the findings and recommendations made during the interviews.

Appendix D: Notes Managing social engineering risk

Enterprise risk management

The proposed social engineering risk management model is based on elements of Enterprise Risk Management Integrated Framework of the Committee Of Sponsoring Organizations of the Treadway commission (COSO) as well as insights from other literature. An adaptation of the models has been made to social engineering risk and generalized to be applicable to all information and not only to IT.

ERM framework

The definition of social engineering risk management reveals the relation to the three dimensions of the ERM framework; it is an ongoing process throughout the *organization*, involves all people within the organization and is able to identify and *manage social engineering risk* to achieve *set objectives*.

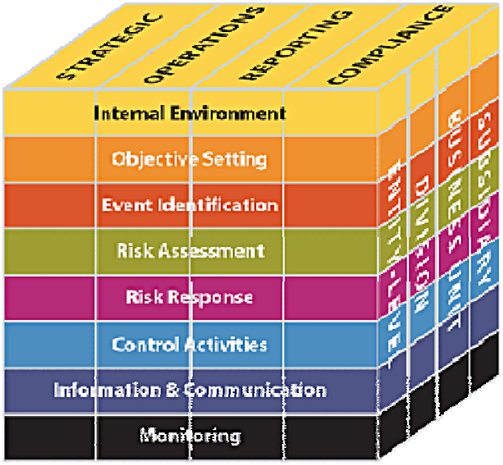


Figure 15: COSO Enterprise Risk Management Internal Framework

Dimension 1: The organizational layer

The risk management process can focus on several layers in the organization. The ERM framework identifies four layers: [COS04]

- *Entity-level* encompasses the entire organization.
- *Division* consists of the departments of the organization.
- *Business unit* consists of the different units within a department.
- *Subsidiary* consists of supporting units within the business unit or other organizational unit.

These layers are chosen because different risk management can take place on these different layers. This is however only a limited set of possibilities, as an organization may consist of many more.

Dimension 2: Organizational objectives

Risk management is implemented to support the achievement of organizational objectives. This dimension of the ERM framework also consists of four categories: [COS04]

- *Strategic* objectives state high-level goals related to the organizations vision and mission.
- *Operations* objectives state the effective and efficient use of the organizations resources.
- *Reporting* objectives state the reliability of reporting.
- *Compliance* objectives state the compliance with applicable laws and regulations.

These objectives all state goals the organization wishes to achieve and are not mutually exclusive as an objective can be related to more categories.

Dimension 3: Components of the management process

The ERM framework also states eight components of the risk management process:

- *Internal environment* consists of describing the (security) organization, for example the security culture, relevant policy and the environment influencing these.
- *Objective setting* focuses on the objectives of the risk management process. These need to be in line with the organizational objectives -the second dimension- and the defined security level.
- *Event identification* consists of the identification of opportunities and risks -internal and external- which influence the organizational and security objectives.
- *Risk assessment* consists of analyzing risks according to their likelihood and impact to see which risks are most eminent and need to be mitigated.
- *Risk response* consists of choosing a response to the risk; avoiding, accepting, reducing or sharing. Depending on this response action needs to be taken. The implemented measures -actions- need to lower risk to the set security level.
- *Control activities* are policies and procedures to support the measures are carried out.
- *Information and communication* are very important as all relevant people need to be informed timely and clearly to support the entire process.
- *Monitoring* consists of (periodic) evaluation and monitoring of the risk management process as implemented. When necessary this can lead to new analysis and possibly changes in for example risk response.

These components form the steps of the social engineering management model and are elaborated on in chapter 7: ‘Social engineering risk management’.