The Defense and Popularity of Social Engineering in Norway

Ernst Kristian Henningsen

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2013

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

The Defense and Popularity of Social Engineering in Norway

Ernst Kristian Henningsen

2013/06/02

Abstract

Social Engineers attack the weakest link in an organization's barrier - it's human users. They do this by manipulating the users into performing actions they wouldn't normally perform. This can have devastating consequences for an organization. The goal may be to get unauthorized access to sensitive information, or gain access to restricted areas, like server rooms. While crackers use their technical skills to break into a computer system and retrieve a password, the Social Engineer use his social skills to make an individual reveal the password themselves.

While there has been written books and papers on different attack vectors, and even some methods for defending against this threat, they are not considered scientific - they are in many cases the experience and views of one particular individual. The amount of scientific work on Social Engineering do not appear to be comprehensive. This Thesis has gathered the essence of what different authors has conveyed about Social Engineering attacks and defenses, as well as why it actually works.

Further it has investigated how popular Social Engineering is in Norway, what vector of attacks are most common and effective, as well as what defense mechanisms one should implement to stand strong against these threats. This has primarily been done by the development of a Questionnaire targeting Norwegian Organizations, a review of existing literature and research, as well as some preliminary interviews with Information Security Professionals.

The results suggest that: (i) Social Engineering by E-Mail is by far the most heavily used vector of attack, followed by attacks originating from websites (ii) most Organizations have mechanisms to defend against Social Engineering, (iii) Organizations conceived Security Risk of Social Engineering is leaning towards medium-high and (iv) the ultimate economic consequences due to Social Engineering attacks are loss of millions of NOK.

Further, not surprising, the review of earlier literature and research, as well as data gathered from our Questionnaire, suggest that Security Awareness is a very important factor for defending against Social Engineering.

We end the Thesis by discussing important steps when developing Security Awareness programs.

Sammendrag

Sosiale Manipulatorer angriper det svakeste leddet i en organisasjon's barriere - brukerne. De gjør dette ved å manipulere brukerne til å utføre handlinger de normalt ikke ville utført. Dette kan ha katastrofale konsekvenser for en organisasjon. Målet kan være å få uautorisert tilgang til sensitiv informasjon, eller tilgang til begrensede områder, som serverrom. Crackere bruker sine tekniske ferdigheter til å bryte seg inn i datasystem for å hente ut passord. Sosiale Manipulatorer derimot, bruker sine sosiale ferdigheter til å få en bruker til å avsløre passordet selv.

Mens det har blitt skrevet bøker og artikler om ulike angrepsvektorer, såvel om hvordan å forsvare seg mot denne trusselen, er de ikke ansett som å være vitenskapelige - de er i mange tilfeller erfaringer og synspunkter til en bestemt person. Mengden av vitenskapelig arbeid på Sosial Manipulasjon virker ikke til å være tilstrekkelig. Denne oppgaven har samlet essensen av hva ulike forfattere har formidlet om angrep og forsvar innen Sosial Manipulasjon, samt hvorfor angrepsformen faktisk fungerer.

Videre har oppgaven undersøkt hvor populær Sosial Manipulasjon er i Norge, hvilke angrepsvektorer som er de mest vanlige og effektive, samt hvilke forsvarsmekanismer en bør iverksette for å stå imot disse truslene. Dette har først og fremst blitt gjort ved utvikling av et spørreskjema rettet mot norske organisasjoner, en gjennomgang av eksisterende litteratur og forskning, samt noen forberedende intervju med fagfolk innen informasjonssikkerhet.

Resultatene tyder på at: (i) Sosial Manipulasjon via e-post er den desidert mest brukte angrepsvektoren, etterfulgt av angrep gjennom websider (ii) De fleste organisasjoner har mekanismer for å forsvare seg mot Sosial Manipulasjon, (iii) Organisasjoners oppfattede risiko av Sosial Manipulasjon lener seg mot middels til høy og (iv) Den ultimate økonomiske konsekvensen som følge av Sosial Manipulasjon er tap av millioner av kroner.

Videre, ikke overraskende, tyder gjennomgangen av tidligere litteratur og forskning, samt analyse av data fra spørreskjema, på at bevissthet innen sikkerhet er en svært viktig faktor for å forsvare seg mot Sosial Manipulasjon.

Oppgaven avsluttes med en diskusjon rundt viktige punkt en bør tenke på når en lager kampanjer for å øke bevissthet rundt sikkerhet.

Preface

I would like to thank my supervisor Finn Olav Sveen for great support when needed.
Further I would like to thank Tore Åsen-Grøssereid and Gunn Marie Henningsen for proof-reading my Thesis. I appreciate my family and friends for keeping to encourage me finalize this Master Thesis, and the Master Degree as a whole.

A special thanks goes to my fellow remote Master students; Roger Larsen and Aud Gran. All of our Skype-sessions these years, for not to mention our regular social dinings at the Mongolian restaurant in Gjøvik, have really made it much more manageable finalizing the degree. Thanks!

Lastly I would of course also like to thank all our respondents for committing their time to participate in our survey, as well as Øivind Høiem and Christian Jacobsen, taking their time to be interviewed regarding Social Engineering.

Contents

List of Figures

List of Tables

1 Introduction

We have all been stopped in the street by someone giving us a tiny gift, for instance a small water-bottle, feeling instantly that we must give something in return. This usually ends up in taking the time to listen on what the person giving us the water-bottle has to say. A dear friend once told a little story about how he himself came victim to a similar case. He had stayed the night at a hotel, of which turned out be be an unpleasant one. He manned himself up to let the reception know what he felt about this particular stay. Determined as he was, he asked to speak with the supervisor of the receptionist. Out the supervisor came, and she instantly brought forward an *apple* asking my friend as she smiled: "Do you want an apple?". My friend took the apple and went away smiling.

This is not much different from making someone revealing to you their password - in both scenarios one get the "victim" to act in a desired way by taking advantage of certain psychological principles. Social Engineering is happening all the time; when your kids for the 50th time starts to cry because he/she knows you will give him an icecream, when we put on a smile so those at work think we are happy as usual, or when deliberately being angry when talking with support on the phone so that they understands the seriousness of your inquiry, or deliberately being very nice to support so that they *want* to help you. However, this Thesis has dived into the more disastrous and malicious aspects of Social Engineering, those that use this way of manipulation to acquire money, information, or even physical items.

Some would say that Social Engineers is only a fancy term for scam-artist, and there may be some truth to that. However, using *Social* and *Engineering* put together also pinpoint what the term is actually about - to *play* with Social Theories.

Social Engineering (SE) has been an vector of attack for decades. The well-known hacker Kevin Mitnick[1, 2] for instance, gained unauthorised access to several assets, by just talking with the right people, at the right time, *in the right way*. History tells of several similar events, where people, and then often end-users, have been fooled into doing something they shouldn't. It is easy blaming the users in such an event. However, the adversaries utilize techniques which make it hard spotting that an attack is in progress, for instance malicious websites made to look exactly like a legitimate one, tricking users to give up sensitive information, like login-credentials. Even if being very skilled and having much knowledge about these sort of attacks, it may be challenging distinguishing fake from real. If the police knocks on your door, you may dare to ask them for ID, but the majority of us is probably not that involved in police-business that we can distinguish real IDs from fake.

1.1 Topic

This project has investigated why Social Engineering works, how popular this vector of attack is in Norway, the different attack-vectors of Social Engineering, the possible consequences of them, as well as how one can defend against them.

Some psychological[1][3] aspects has be covered, to better understand why Social Engineering work as an vector of attack. Such as Robert B. Cialdini's *Six basic tendencies of human nature*[4]. Some technical attacks has been mentioned, as they are often combined with Social Engineering attacks. This could for instance be phishing emails, or "free" (malicious) USB-sticks delivered to an Organisation.

1.2 Keywords

Information Security, Attack, Defense, Intruders, Social Engineering, Human Hacking, Misusing trust, Manipulation, Security Awareness

1.3 Problem description

Humans are naive, and with good reason. As a society we need to be able to trust each other. There exist however adversaries that feed on this naivety for personal gain. This may be done by using a wide repertoire of attack-vectors, such as phishing, spear-phising[2] [5], phoning, physical letters, "free" USB-sticks (infected with malware) and face-to-face communication to mention a few. They all have in common, in light of Social Engineering, that they exploit the naivety in us all.

Implementing procedures for defending against attacks can be a hard nut to crack, and if not done, will likely result in economic loss. Look for instance on the article "Measuring the Effectiveness of In-the-Wild Phishing Attacks",December 2009[6], written by the firm Trusteer, where they state, that for every million of bank-clients, the annual losses in regard to phishing attacks is estimated to be between 2,4 million and 9,4 million dollars.
If this would be correct for Norway as well, and we estimate that 3,3 million Norwegians use online banks[7], we would stand before an average annual loss of almost 20 million dollars, roughly 115 million NOK's - and this would only be due to automated phishing attacks. Focus on awareness training could very likely reduce this loss.

Though nevertheless the economic loss just mentioned, the daily phishing-mails that request you, in poorly written language, to give up your password or similar, is not the security risk to worry about; it is those mails only sent to a couple of individuals, written in perfect grammar, specifically targeted towards the recipient, that should be in focus. These can be hard to detect and have potentially a much bigger impact on an organization. Manually analysing every single email for potential malicious intentions would of course consume to many man-hours to be feasible in practise. So how do one attack such a problem? What if we weren't talking about mail,

[1] "Psychology is the study of mind and behaviour.". The University of New South Wales, Sydney, Australia
[2] Spear Phishing is phishing-attacks that are tailored towards specific individuals[5]

but an individual requesting access to an organization's server room? Would one treat this any differently?

A survey performed by the well-known company Checkpoint[8], released in September 2011, state that roughly half of every business has suffered from at least 25 social engineering attacks the last two years, with each costing between 25 000 and 100 000 dollars. The survey was performed on 853 IT professionals. This indeed tells us that Social Engineering is a very costly affair for victims of it. The survey not only shows that this kind of attacks is motivated by financial gain, but also out of revenge.

Beneath in figure 1 one find an example of Christian Jacobsen[3] gaining access to a higher security zone in a Social Engineering test. When someone opens the door, the cable will flip over and prevent it from closing. Who will be suspicious of someone walking around with a short cable and tape?

Figure 1: Gaining access by a short cable and tape

[3]Christian Jacobsen is known within the Security Community in Norway, where he has held several interesting presentations about Social Engineering and its possible impact on company assets

1.4 Justification, motivation and benefits

Social Engineering takes advantage of the human aspect of Information Security to infiltrate a system. Where we have highly skilled IT professionals maintaining technical equipment that defend us against technical attacks, attacks on end-users have no professional defences at all. Instead every user is left defending themselves. It is typically hard enough for someone skilled in the matter revealing an attack in progress, that we can certainly not expect end-users to do so - unless we can improve their awareness of Social Engineering attacks, so they become better at calling them out. It is therefore important looking at what attacks that exist and are most used, as well as how one can defend against them. This will help making user-awareness programs more efficient.

If users become more robust against these attacks it will likely result in less money lost for the Organisation, as well as higher confidence among the employees. But before investing vast amount of resources in defending against Social Engineering - is it really happening here in Norway? Should we expect such attacks to happen in the future towards Norwegian Organizations?

1.5 Research questions

- Why does Social Engineering work?
- How popular is Social Engineering as an vector of attack in Norway?
- What are the common and effective Social Engineering methods today?
- How can an Organization defend itself against Social Engineering?

1.6 Contributions

This Thesis helps to understand Social Engineering as a threat, what it really is about. It shows why it is not sufficient only relying on technical controls to defend one's organization, but that one also need to consider the more non-technical approach for defending, *hardening* the employees. Further, it has investigated how popular Social Engineering is as a vector of attack in Norway and may therefore work as an incentive for management in organizations to invest more/less resources into defending against Social Engineering, depending on their risk-profile. The results show that the consequences of Social Engineering can be major, in terms of millions of Norwegian Kroner.

Further the Thesis suggest what kind of Social Engineering attacks, *which are detected*, are often used to get access to sensitive information/assets of a system/Organisation. It has identified some of actions one can take to defend against Social Engineering, helping to reduce economic losses.

1.7 Thesis outline

- Chapter 2 presents what we know about Social Engineering, discussing various literature and studies been made on the topic, as well as providing insight into *why* Social Engi-

neering actually works. The chapter ends with a few real-life examples being published by media in the latest past.

- Chapter 3 presents and discusses the various research methods we have chosen to use for our Thesis, as well as ethical perspectives to consider
- Chapter 4 presents how we designed our Questionnaire
- Chapter 5 presents and discusses the results from our Questionnaire
- Chapter 6 discusses how to defend against Social Engineering, including input from books, articles, earlier research, interviews as well as the results from our Questionnaire
- Chapter 7 discusses how one can/should develop and conduct a Security Awareness Program
- Chapter 8 summarized the content of the Thesis, what we believe are the most important findings
- Chapter 9 presents some of the work that could be interesting pursuing further, we amongst other propose the concept of a Framework for developing Security Awareness Programs

We now proceed by presenting what we know about Social Engineering.

2 What we know about Social Engineering

It do not seem to exist extensive amount of scientific resources on the topic of Social Engineering. There exist however a vast amount of non-scientific sources, like books, articles and quotes from security experts (and non-experts), that claim to shed light on why Social Engineering work, different vectors of attack, as well as how to defend oneself against Social Engineering. They typically include real-life examples and scenarios of Social Engineering attacks. A challenge is distinguishing high validity sources from those with low validity.

Similar to other types of attacks, one can split Social Engineering into different *phases* (by some referred to as the *Social Engineering Cycle*):

- Gathering information
- Developing trust
- Exploiting trust
- Goal reached

A visual representation is found in the figure below, made by Malcolm Allen.

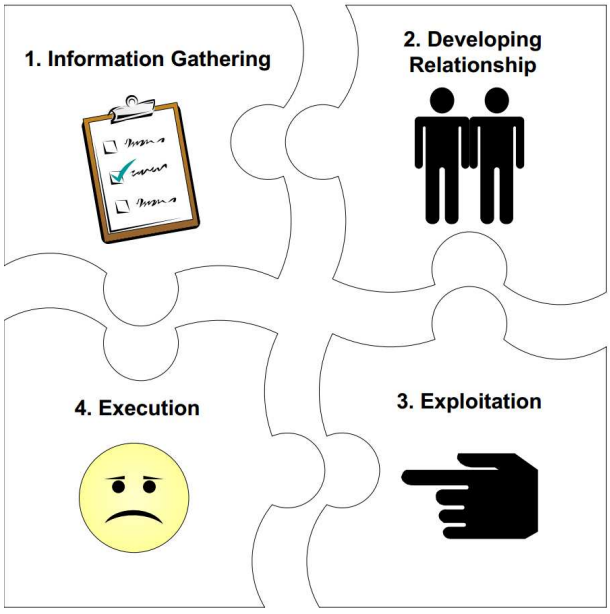

Figure 2: Social Engineering Cycle. Figure made by Malcolm Allen and published through SANS, 2007

One of the core necessity for Social Engineering being successful, is trust. Trusting that the E-Mail received is from a legitimate source, trusting that the cleaning personnel actually are there to clean, and that support currently calling, is calling to support you with something.

To appear trustworthy, information is important. Information that in some way is tied to the victim. Ultimately one use this information to complete one's goal, which could be anything from gathering credit card information to stealing physical blueprints of a new product. Though as it is very unlikely that one can manage this by only passively gathering information, one usually need to retrieve information that makes one *appear* to have the authorization needed to access certain information or objects. This is where the *Multi-tiered Social Engineering* concept,presented by social-engineer.org, make it's way.

As just mentioned, the Social Engineer needs to seem trustworthy and legit. In order to do so he need to present information that *should* only be known to the real identity. Retrieving some *perceived low-value information* from a helpdesk, the Social Engineer can use this information to gather more information at a later point, because he already knows *something*. Quoted below from social-engineer.org[9], the concept of a *Multi-tiered Social Engineering attack*:

1. Attacker has [xyz] info
2. Attacker uses [xyz] to socially engineer Company A into giving [abc] info
3. Attacker uses [abc] to socially engineer Company B into giving [mno] info
4. Attacker uses [xyz], [abc], and [mno] info to gain access to account in Company C

This is one of the reasons why Social Engineering can be so dangerous. One do not only gather potentially sensitive information along the way, one also distribute the risk taken between all contact-points. Unless these contact-points speak to each other, chances are slim that the dots will be connected, and the attack is more likely to be successful - without detection.

We now continue by discussing why Social Engineering works.

2.1 Why Social Engineering work

"*It all depends on how we look at things, and not on how they are themselves*"
- Carl Gustav Jung

One interesting observation made by Christian Jacobsen while conducting Social Engineering tests, when working for the IT-Security company Secode, is why there sometimes in human reasoning, exist a logical flaw in decision making. This applies to Social Engineering in that one may not let a person entering from the main-entrance of a building gain access to a higher security zone, but when that same persons enters from another environment, but from the same security-zone, for instance the restrooms, the person would gain access.

When looking into *why* Social Engineering work one could just say that we humans are naive. That is however to broad and simple accepting as a viable answer. We need to address the underlying principles one actually take advantage of when manipulating someone. Most literature that discuss Social Engineering, also present something about why it works as well.

A different approach than studying relevant literature and research, could be to interview psychiatrists regarding principles of influence, and why we may be as prone to manipulation as we are. Though likely showed to be valuable, we could not commit to conduct such interviews. This because we had limited time conducting our thesis, and most time available needed to be put into the development, administration and analysis of the Questionnaire investigating the popularity of Social Engineering in Norway. We therefore proceeded by mainly relying on earlier research and literature.

It is important remembering that there seldom exist one way of approach that influence every human the same. We all react/behave differently in different situations, based on personality, prior experience and knowledge, and even current mood.

Bruce Schneier try to shed light on how the inhabitants of a society are somewhat *bound* by various principles into behaving as the society want us to behave, in his book Liars & Outliars[10] released in 2012. Below in figure3, one find Bruce Schneier's graph *Societal Pressures and their relations* retrieved from the book. Take a moment studying the graph; the figure suggest various pressures, norms and interests that we consider when choosing whether to cooperate (say yes) to a request, or defect (say no) to a request.

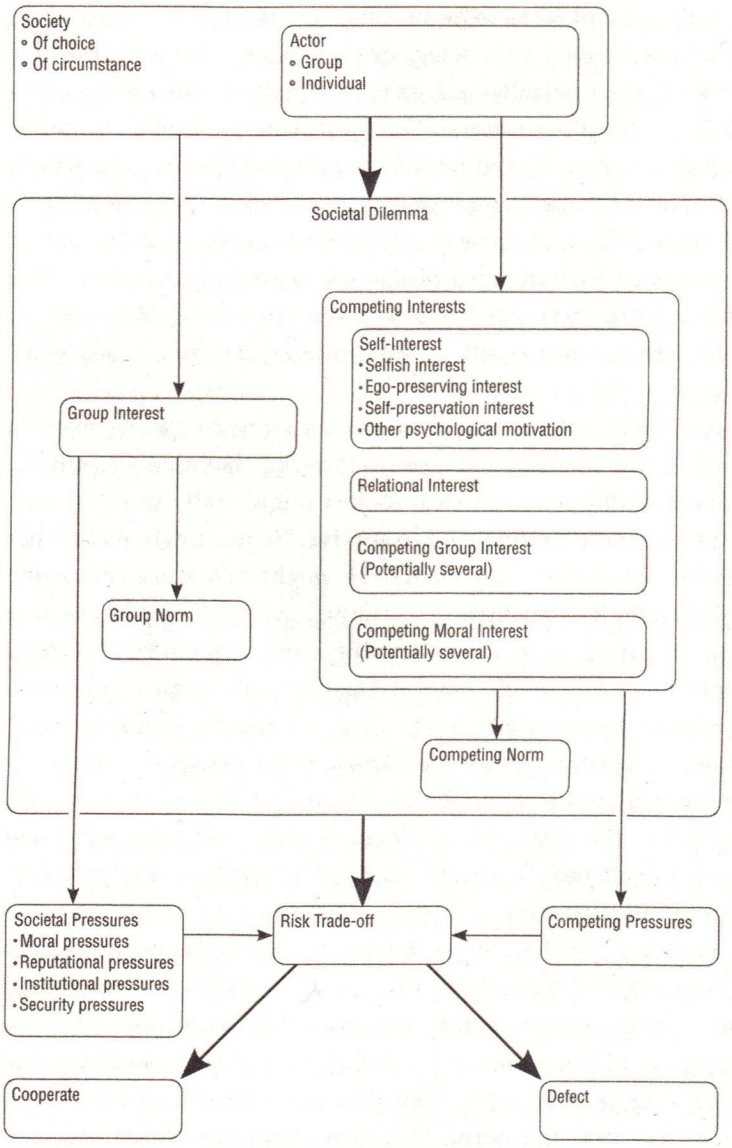

Figure 3: Societal Pressures and their relations

No scientific resources have been located that addressed Social Engineering as a whole in regard to why it works. However, a paper published at ieee.org addressing why *Phishing* (a technique used by Social Engineers) works has been discovered.

The paper, written by Jingguo Wang in August 2012, titled *Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email*[11], addresses how individuals process phishing emails and how they decide how they respond to it. More specifically, as Wang states, the study

> examines how users' attention to "visual triggers" and "phishing deception indicators" influ-

> ence their decision-making processes and consequently their decisions.

He conducted a survey in which he used a real phishing email as *stimules* towards 321 members of a public university community in North-east US. As a conclusion he states:

> Knowledge of email-based scams increases attention to phishing deception indicators, and directly decreases response likelihood.

In other words, the study suggest that Security Awareness is one of the catalysts for defending against such threats.

If looking more broadly however, and not using the particular term of Social Engineering, one find a paper written by Ames et al. in 2002 titled *A system and method for enhanced psychophysiological detection of deception*[12]. They say, quoting:

> In practice, a major difficulty with the reliability and validity of any lie detection technique is the extreme subjectivity of interpretation
> ....
> By base-lining how an individual processes information for lies and truths, and correlating these signatures with other micro-dynamics cues, a more accurate description of the deception can be established.

This concept of *base-lining* is also present in the fiction-serie *Lie To Me*, where the main-character, Cal Lightman, being the worlds greatest expert in detecting lies, analyzed body-language and *microexpressions*[1]. Usually he would make a base-line of peoples behaviour when telling the truth, for then observing if they behaved any different when answering certain questions. If they did, it could be an indication of them lying.

Though being fiction, the serie is based upon documented research done by Dr. Paul Ekman. He is well known for his studies on microexpressions. Micro-expressions are expressions that are not easily controllable and occur in reaction to emotions. These expressions can last for as short as one-twenty-fifth of a second[14]. Dr. Ekman has identified seven different basic emotions: *Anger, Disgust, Fear, Joy, Sadness, Surprise and Contempt*. Below is an example of six of these emotions, as shown by Tim Roth in the role as Cal Lightman in the serie Lie To Me as just mentioned.

[1] A microexpression is a brief, involuntary facial expression shown on the face of humans according to emotions experienced.[13]

Figure 4: The Microexpressions shown by Tim Roth in his role as Cal Lightman in Lie To Me

Christopher Hadnagy wrote in 2010 a book titled *Social Engineering - The Art of Human Hacking*[14]. In it he suggest explanations to why Social Engineering works, and suggest two main methods on how to use microexpressions for malicious intent:

- Using Micro-expressions to elicit or cause an emotion
- Using Micro-expressions to detect deceit

As told by Hadnagy, a study called *Neural and Behavioral Evidence for Affective Priming of Unconsciously Perceived Emotional Facial Expressions and the Influence of Trait Anxiety*[15], by Li et al. showed that if a person observed these short micro-expressions, the person itself would for a short period be in the emotional state as observed. (Observing the micro-expression sadness would make the person sad for a brief moment). Quoting Hadnagy:

> Learning to exhibit the subtle hints of these ME can cause the neurons in your target's brain to mirror the emotional state they feel you are displaying, making your target more willing to comply with your request.

Despite for a good cause, it is likely not randomly chosen when young and poor kids on television are shown staring sadly into the camera. It makes us feel sad too, increasing the likelihood of people opening their wallets to support them. This is of course the more legitimate uses of such manipulation, but what if you find a person being upset just outside the back entrance of your organization (often used by smokers), in which the person claims to have forgotten both his/her access-card and mobile inside - are you helpful and let the person in?

Deception Detection - Project Hostile Intent

Though not explicitly building on microexpressions, the Department of Homeland Security has launched a project called *Hostile Intent*, which aims to identify individuals having hostile intentions towards United states[16, 17], by looking at behavioural and speech cues.

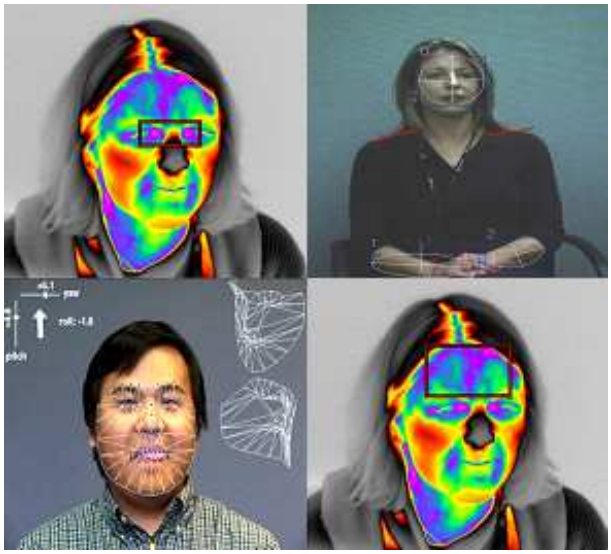

Figure 5: Picture retrieved from www.dhs.gov: Project Hostile Intent

Hadnagy do not only mention microexpressions when trying to explain why SE work. Though other parts do not seem to be sufficiently based on documented and proven theories, making us question the validity of what is described. Hadnagy is of course not the only author describing such *hypothesises*; several professionals make an effort describing why or how, which may, or may not be based on proven theories. Though if these descriptions were to work as stated, it sounds like something *everyone* should learn, as it would make communication with other human beings easier. Two examples are:

- Three Main Modes of Thinking - if speaking in the same *mode* as another person, one is more likely understand each other correctly
  - Sight, or a visual thinker - *That looks good to me*
  - Hearing, or an auditory thinker - *That sounds good to me*
  - Feeling, or a kinesthetic thinker - *That feels good to me*

- Neuro-lingustic Programming

Neuro-linguistic Programming (NLP) has in fact been subject to quite some negative sayings, for instance being considered as *pseudo-science*[2].

The Neuro-linguistic programming concept involves amongst others, *rapport* and *matching*, as suggested by Mo Shapiro, in his book *Successful Neuro-Linguistic Programming in a week*. Below a quotation retrieved directly from the book:

> - Rapport - The process of building and sustaining a relationship of mutual trust, harmony and understanding. This happens through matching the accessing cues from words, eye movements and body language. (Not quote: Hadnagy state the concept "Kill them with kindness", being kind to people, is a quick way to build rapport)
> - Matching - Rapport is partly established by *matching* the representational systems and body language of others. This might mean sitting down if they are seated, breathing slowly like them or speaking at a fast pace with them. They will have the sense that you are 'with and for' them rather than against them. The advantage of matching is that the other person recognizes at an unconscious level that you understand and value what they are communicating. It will also help you unconsciously to join in genuinely with their understanding.

Shapiro further tells that in some occasions one may take advantage of *Mismatching*. If this were to be proven theories, in a Social Engineering endeavour, mismatching could be used to make sure that a victim, or someone else, do not interfere with "the mission".

In 2009, Nathaniel Joseph Evans wrote a Dissertation titled *Information technology social engineering: an academic definition and study of social engineering - analyzing the human firewall*[18]. He did an extensive effort into locating existing literature on the topic of Social Engineering. He also discussed Neuro-linguistic Programming (NLP) as a principle of why Social Engineering works, and how one may use it for malicious intent. He neither seem to provide evidences for NLP actually working as stated, in terms of being scientifically proven as a theory.

The techniques and thoughts that NLP represents may of course have been successfully executed in several occasions, but without a scientific and neutral study on the phenomenons one cannot treat it as known theories, but rather hypothesises. The concept of NLP was originally developed by Richard Bandler [19, 20], and John Grinder [21, 22] in the 1970s . Several studies[23, 24, 25, 26, 27], as mentioned in the article *Selected Alternative Training Techniques in HRD*[28], written by Bergen et al. (1997), has been made regarding elements of NLP. Though quite old, latest being 1988, they all conclude with there being insufficient evidence for NLP actually working as stated. Further, Bergen et al. said, quoting:

> Bandler and Grinder stated that they were not interested in establishing scientific validation of NLP but instead intended to portray what works.

There exist a lot of practitioners and trainers of NLP. Some debate that studies of NLP just have been subject to poorly explained scientific methods and similar, and that it is almost just coincidental that no studies *which have been performed*, has been accepted as valid by researchers world wide. Steve Andreas mentions in his blog about NLP[29] a project called *Research & Recognition Project*, which aims to support scientific research of NLP:

[2] Pseudo-science are for instance hypothesises presented as validated scientific theories, but in fact has not been proven as such.

> The overall mission of the Research and Recognition Project is to support, coordinate, and fund rigorous scientific research in the field of NLP and related intervention strategies.

For those particularly interested in proving NLP as a theory, one should perhaps turn towards this project for funding.

Tendencies of Human Nature

Kevin D. Mitnick also suggest principles of why Social Engineering work in his book *The Art of Deception - Controlling the Human Element of Security[30] (2003)*. He points out some of the *Human tendencies*[3] that Professor Robert B. Cialdini discusses, in his book *Influence - Science and practise*[4]. Cialdini presents possible explanations on why we humans react as we do on influence. He presents *six basic tendencies of human nature*. Below is a short explanation of these tendencies extracted from *The Art of Deception*[30], by Mitnick. Cialdini base these principles on studies performed by other researchers. Hadnagy does as well discuss these principles in his book [14]

- **Authority** - A person can be convinced to comply with a request if he or she believes the requester is a person in authority or a person who is authorised to make such a request. Study: Obedience to Authority, S. Milgram, 1974
- **Liking** - People have a tendency to comply when the person making a request has been able to establish himself as likeable, or as having similar interests, beliefs, and attitudes as the victim.
- **Reciprocation** - We may automatically comply with a request when we have been given or promised something of value. When someone has done something for you, you feel an inclination to reciprocate. This strong tendency to reciprocate exists even in situations where the person giving the gift hasn't asked for it.
- **Consistency** - People have the tendency to comply after having made a public commitment or endorsement for a cause. Once we have promised we will do something, we don't want to appear untrustworthy or undesirable and will tend to follow through in order to be consistent with our statement or promise.
- **Social Validation** - People have the tendency to comply, when doing so appears to be in line with what others are doing. The action of others is accepted as validation that the behaviour in question is the correct and appropriate action.
- **Scarcity** - People have the tendency to comply when it is believed that the object sought is in short supply and others are competing for it, or that it is available only for a short period of time. Study: Increasing the attractiveness of college cafeteria food, S.G. West, 1975.

Everybody can use these tendencies for their own benefit, and likely everybody are, if not with intent, then unconsciously, in some way or another. However, using these tendencies in Social Engineering is likely to cause much more harm than "forcing" a person to listen on what one

[3] Cialdini has presented six Human Tendencies; Authority, Liking, Reciprocation, Consistency, Social Validation and Scarcity, that says something about why we humans react on influence as we do

has to say for two minutes.

As mentioned, Cialdini base his principles on related studies mostly conducted by other researchers.

One of the studies addressing the principle just described, is *Obedience to Authority*, conducted by Stanley Milgram in the 1960's. This study showed that most people obey authority, regardless of the consequences of doing so.

In the experiment, an authoritative person (being the experimenter for that experiment) ordered the participants to give electric shocks to another person. The shocks would get stronger and stronger, ultimately killing the person receiving them. The participants went to great length obeying the experimenter, despite seeing the person electrocuted being in a lot of pain (this was however not truly the case - the person faked being in pain and was part of the experiment).

It is easy "turning on" *auto-pilot* when speaking with authoritative figures, and just do as they tell us. We expect they have the necessary background to make the correct decision in a given context. The problem however, is when adversaries take advantage of this principle and use it with malicious intentions.

An example of this could be to show up in a policy/fire-fighter-uniform, stating reports of a situation occurring from inside the organization has been received and needs urgent attention. Further one would state that if access is not granted, one risk being criminally accused for the obstruction of Justice. Throw in someone speaking authoritatively on the outside in a megaphone and one may be granted access.
Lisman et al. discuss the concept of auto-pilot, more specifically the relation between the *unconscious/conscious* part in the mind, and *habit/non-habit system*, in their paper *The pilot and autopilot within our mind-brain connection*[31].

Below, in figure6, on find the *cycle of reciprocity* as presented in Hadnagy's book.

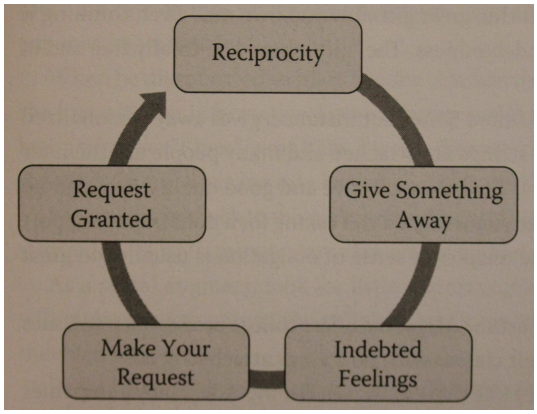

Figure 6: The cycle of reciprocity from Hadnagy's book

2.1.1 Consistency and Inner Commitment

Using the concept of *Consistency* and *Inner Commitment*, as also described by Cialdini, Hadnagy pose a rough example of a phone-conversation he state is often used by solicitors:

> Hello, how are you today?
> I am doing great
> That is good to hear, because some people who are not doing so great can use your help

Please also find the *stages* of this technique in figure 7 below.

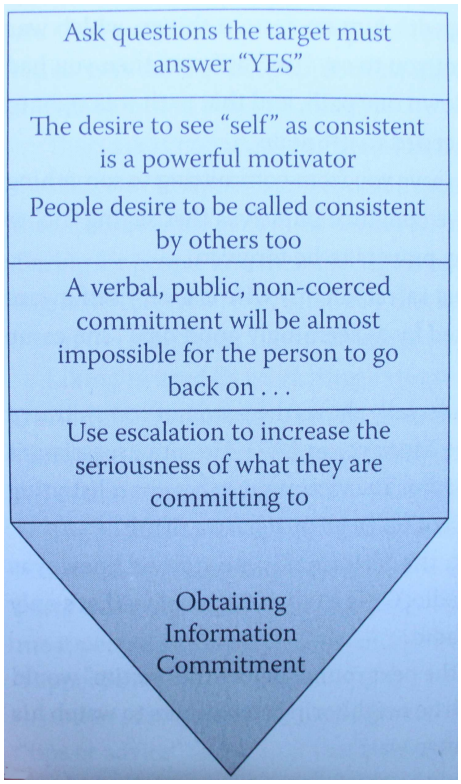

Figure 7: Using Commitment and Consistency to Harvest Information, retrieved from Hadnagy's book

2.2 Social Engineering Techniques

2.2.1 Reverse Social Engineering

SANS mentions in *A Multi-Level Defense against Social Engineering*[32] the use of a technique known as *reverse Social Engineering*. It means to produce a problem at the victim's end, for so to go "fix" it. Examples could be power-outage, clogged drains, malware-infections, etc.

2.2.2 Pretexting

Pretexting is a very important part when conducting a Social Engineering attack. It is basically the story on which argument for making the request one do, for instance: I am here *to fix the faulty server*, therefore I need access to the server-room. Or, I am here *to fix the clogged toilet*. Christian Jacobsen also points out the importance of giving a *reason* for being in a certain environment. The validity of the reason is not that important, as long as a reason is given, he says.

Hadnagy points out that pretexting is more than just lying to a victim. It may involve creating a whole new identity to manipulate a victim to comply to one's request.

2.2.3 Gathering Information

There exist several approaches to gathering information about a target. Some of which are presented below.

- Shoulder-surfing - Much information, for not to say *up-to-date* information may be retrieved by looking at peoples screen when working at the bus, train, plane and etc. There exist so called "privacy screens" one can attach to most screens, whether it is a laptop, tablet or phone. What these screens do is to limit the *angle* in which a screen is visible.
- Dumpster diving - Considers going through the trash for information that can be used to establish trust.
- Tailgating - Following an employee of an organization when he or she unlocks a door.

Google

Google (and other search-engines) can reveal very much relevant information when conducting a Social Engineering attack. Basically one can use the same method as mentioned earlier about *Multi-tiered Social Engineering*. One may for instance search for a name and get a phonenumber. Searching on this phonenumber may reveal an email-address. Searching on this email-address may yield another email-address and so on. One just need to find out what *connect the dots*.

Company Website

Most company websites has much information available regarding contact-points and similar. One may often also retrieve the *format* of their email-addresses. (Some use "Firstname"."Lastname"@"Domain", others may use the opposite and variations of it. Knowing this one may guess a person's email-address.

BRREG.no

This site holds information of all Norwegian companies and organizations. It may be their organization-number, a phonenumber for contacting a specific person, and the name of this person.

Facebook

Many people share almost everything of their life on Facebook - a goldmine of information of which one can use to build trust with any individual. "We like the same music - let's be friends".

Compromised systems

Listening in on what is assumed to be private conversations in between participants, may reveal a lot of beneficial and company-confidential information. If able to compromise a computer or phone, one instantly have access to internal/confidential information that if not valuable itself, can be used to escalate further into an organization.

Maltego

As described on paterva.com:

> Maltego is a program that can be used to determine the relationships and real world links between:
>
> - People
> - Groups of people (social networks)
> - Companies
> - Organizations
> - Web sites
> - Internet infrastructure such as:
>   - Domains
>   - DNS names
>   - Netblocks
>   - IP ad dresses
> - Phrases
> - Affiliations
> - Documents and files

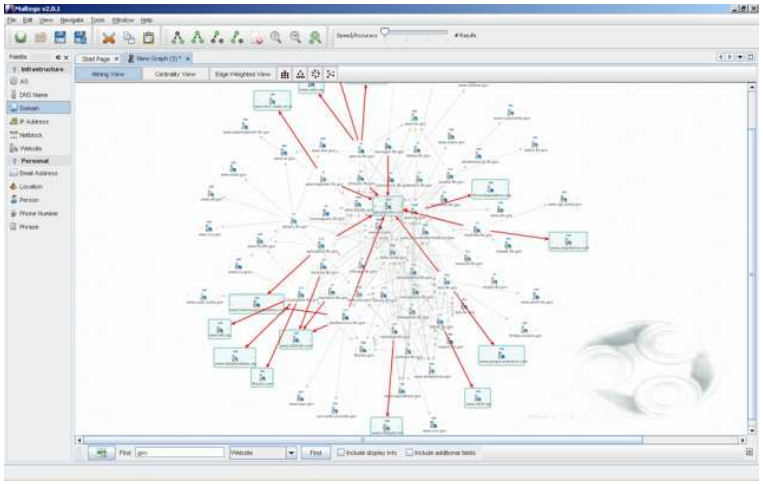

Figure 8: Example of Maltego, retrieved from social-engineer.org

Maltego may be used when technically penetrating an organization as it visually reveals what certain hosts exists, as well as how they are connected. It may however also be used by Social Engineers to see relations that otherwise would not be as apparent (if not using a similar tool).

Social Engineering Toolkit (SET)

On www.social-engineer.org one can find the Social Engineering Toolkit (SET) . This is a toolkit specifically made to help perform penetration tests aimed towards humans.

```
root@bt:/pentest/exploits/set# ./set

  [---]       The Social-Engineer Toolkit (SET)          [---]
  [---]        Written by David Kennedy (ReL1K)          [---]
  [---]                Version: 0.7                      [---]
  [---]             Codename: 'Swagger Wagon'            [---]
  [---]     Report bugs to: davek@social-engineer.org    [---]
  [---]        Java Applet Written by: Thomas Werth      [---]
  [---]        Homepage: http://www.secmaniac.com        [---]
  [---]     Framework: http://www.social-engineer.org    [---]
  [---]       Over 1 million downloads and counting.     [---]

   Welcome to the Social-Engineer Toolkit (SET). Your one
    stop shop for all of your social-engineering needs..

            Follow me on Twitter: dave_rel1k

     DerbyCon 2011 Sep29-Oct02 - A new era begins...
  irc.freenode.net - #DerbyCon - http://www.derbycon.com

Select from the menu:

1.  Spear-Phishing Attack Vectors
2.  Website Attack Vectors
3.  Infectious Media Generator
4.  Create a Payload and Listener
5.  Mass Mailer Attack
6.  Teensy USB HID Attack Vector
7   Update the Metasploit Framework
8.  Update the Social-Engineer Toolkit
9.  Help, Credits, and About
10. Exit the Social-Engineer Toolkit

Enter your choice: 1

Welcome to the SET E-Mail attack method. This module allows
you to specially craft email messages and send them to a large
(or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure
"Sendmail" is installed (it is installed in BT4) and change
the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting
SET do everything for you (option 1), the second is to create
your own FileFormat payload and use it in your own attack. Either
way, good luck and enjoy!

1. Perform a Mass Email Attack
2. Create a FileFormat Payload
3. Create a Social-Engineering Template
4. Return to Main Menu

Enter your choice:
```

Figure 9: Main Menu of the Social Engineer Toolkit (SET)

2.3 Social Engineering in Media

In the recent past there has been several examples of Social Engineering appearing in media. We present a few below.

Apple Tech Support

At the 3rd of August, 2012, tech reporter Mat Honan's iCloud account was compromised[33]. This resulted in his Ipad, Iphone and MacBook Air being remotely wiped. Some adversary had Socially Manipulated an employee at Apple's Tech into giving access to Honan's iCloud-account. Someone had called AppleCare claiming to be Honan, saying that he were unable to access his email-account. Despite the caller being unable to answer the predefined security questions they issued a temporary password after the adversary had given publicly known information, quoting wired.com[33]

> Amazon tech support gave them the ability to see a piece of information — a partial credit card number — that Apple used to release information. In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification.
> .....
> Apple tech support confirmed to me twice over the weekend that all you need to access someone's AppleID is the associated e-mail address, a credit card number, the billing address, and the last four digits of a credit card on file.

Thief pretended to be ambulance driver

At the 25th of April, 2013, f-b.no informed[34] that a jacket used by ambulance drivers had been stolen. After, the jacket-thief had entered the personnel-room and taken personal effects belonging to the *real* ambulance drivers. Further he had entered the children department of the hospital and stolen a wallet from an employee. People observing this thief, in an ambulance jacket, likely believed that he really was an ambulance driver - why shouldn't they? Further this would likely had given him access to most places an ambulance driver can enter.

Disguised sex offender broke into prison

At the 4th of Mars, 2013, dagbladet.no informed[35] that a person having been convicted of several sexual criminal activities, had used a uniform and false ID-badge to grant himself access to prison-areas. He did not get caught before he started to move prisoners from one cell to another.

Timely email with malicious link

At the 17th of April, 2013, online news-sites reported of a big explosion near Waco in Texas, in a fertilizer plant. At the 18th of April the author of this Thesis received an email with the subject: *CAUGHT ON CAMERA: Fertilizer Plant Explosion Near Waco, Texas*.
The only thing present in the email was the following link : http :// 95. 87. 6. 156 / news. html (spaces included so that one do not accidentally click on it).
Searching for the link on urlquery.net one find relations to malicious sites on the internet. Clicking on the link may therefore result in ones computer being compromised.
This is just an example of how impudent an adversary can be - taking advantage of a sad event like this for personal gain. This should be regarded as a non-targeted attack, were the likelihood for success is increased because of the curiosity of the recipient.

Personal Experience - Auto-Pilot and Airport Security

In several articles in the media one are able to comment under pseudonyms, or avatars. Some make rather harsh comments regarding the intelligence of the victims of scams, or Social Engineering attacks. In some scenarios one may of course wonder how certain individuals can respond as they do, but that is what is scary about Social Engineering. It takes advantage of peoples *auto-pilot*.

A personal experience from myself, the author of this thesis, was in an airport, traversing through the security-control. Randomly chosen a personal body check had to be done. I said to the security guard that I wanted to gather control of my personal effects before continuing with the body check, which I was given permission to. The security guard did however ask of me that I gave him my shoes prior to gathering my personal effects. After the body-check was over, I went to grab my luggage while thinking anxiously; *where is my wallet!?*

Desperately looking for it in the luggage and all possible spaces it could be, I finally asked the security guard if he knew where it was - and he did, he had put it in my shoes, awaiting to be scanned. A master degree within Information Security, professional experience within Information Security, as well as an unconditional interest in the Human aspect of Information Security, combined with being in the process of writing this Master Thesis about Social Engineering, did not "protect" me from for a short while entering the *auto pilot* and just doing what the authoritative security guard asked of me. I did of course afterwards remember that I had given the wallet, but not at the moment when I could not find it.

TV-Series about Social Engineering

For those particularly interested in Social Engineering, not only as to defend against it, but also as possible entertainment, please find in the AppendixA several examples of TV-series touching the topic.

2.4 Common and effective Social Engineering attacks

Methods of performing Social Engineering is almost entirely up to the creativity of the attacker. Though as some will be more effective than others in terms of cost/benefit, revealing these methods could be done by shedding light on what attacks have been reported earlier. Looking at earlier reports it is important remembering that we are likely looking at significant under-reporting, as few businesses enjoy showing their weaknesses. The fourth Quarterly report, published by NorCERT (NSM), in 2011, points out that 1/3 of companies have been hit by computer crime, while only 1% of the incidents have been reported to the police. This can consequently result in methods considered being common, actually are not. Further one must keep in mind that there may exist several attacks that have gone past undetected, consequently resulting in them being unknown, at least as a common method.

Snekkenes et al. performed in 2005 a case study presented in *Measuring Resistance to Social Engineering*[36] The case study investigated how many users would enter their login-credentials

on a seemingly legitimate site. 59 out of 120 participated in the case study, of which 15 gave up their credentials. They argue for the case study showing that Social Engineering *represents a realistic and serious threat*.

Using a seemingly legitimate site to harvest information is often referred to as *phishing*. The article *Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies*[37], written by Aburrous et al. in 2010, discusses some phishing techniques, like phone phishing and website phishing. It also discusses three conducted case studies within phishing with interesting results. They mention the education of user-awareness as an important step when developing defenses, quoting: *Our experimental case studies point to the need for extensive educational campaigns about phishing and other security threats.*

It seems as the literature and studies available mostly consider phishing. Though being a technique used by Social Engineers, we want to gain a broader view on common and effective SE-attacks, towards Norwegian targets/organizations. Being able to do so, we need an approach to gather such data. In the next chapter we continue by adressing appropriate methodology for finding an answer to this, as well as the popularity of SE-attacks in Norway, and how to defend.

3 Methodology

We will now discuss appropriate methodologies for answering three of our research questions; (i) *How popular is Social Engineering as an attack-vector in Norway?*, (ii) *What are the common and effective Social Engineering methods today?* and (iii) *How can an Organization defend itself against Social Engineering?* Our first research questions regarding why Social Engineering works we already have discussed in the prior chapter.

In this chapter regarding Methodology, we discuss each research question separately, and end each discussion by the method(s) we found appropriate, and in which we used to progress with our Thesis. Finally we end this chapter by discussing ethical perspectives of our methods. Afterwards, we extend this chapter by a dedicated chapter surrounding the design of the Questionnaire we chose to develop.

Within the GUC-community[1], a recognized book that addresses research methods, is "Case Study Research - Design and Methods[38] (2009), written by Robert K. Yin. He mention five major research methods, as shown below in table 1:

METHOD	**Form of Research Question**	**Requires Control of Behavioral Events**	**Focuses on Contemporary Events)**
Experiment	how, why?	yes	yes
Survey	who, what, where, how many, how much?	no	yes
Archival Analysis	who, what, where, how many, how much?	no	yes/no
History	how, why?	no	no
Case Study	how, why?	no	yes

Table 1: Relevant Situations for Different Research Methods (COSMOS Corporation)

Yin state one can use each of these research methods for every kind of research problem. He thereafter state three conditions which should be used when choosing an appropriate method: The..

..type of research question posed.
..extent of control an investigator has over actual behavioural events.
..degree of focus on contemporary as opposed to historical events.

He thereafter reference a table (originally made by COSMOS Corporation) giving an overview of suitable methods for answering different research problems (please find it below in table 1). We

[1] GUC: Gjøvik University College

will now proceed by using this table as a basis for discussing, and choosing, appropriate methodologies for our Thesis.

It is imperative interpreting the table correctly. For example, if one's research problem doesn't require control of behavioural events, it doesn't mean that an experiment *cannot* be used. However, if you do require control, out of those five methods, experiments *should generally* be used.

For our Thesis, control of behavioural events are not needed in order to answer any of our research-questions, though this does not rule out any of the research methods in the above table 1.

We proceed by discussing each research question for themselves. We will first discuss whether or not focus on contemporary events are needed to answer the research question, before looking into the *form* of the research question, discussing why certain methods are appropriate or not. Some preliminary Interviews has been conducted to gather important aspects of Social Engineering.

3.1 How popular is Social Engineering as an vector of attack in Norway?

No sources have been found that has investigated the popularity of Social Engineering as a whole in Norway.

Sources regarding cyber-activity, like Trojans, are more present[39, 40]. Though perhaps Social Engineering being the root-cause of infection in some of these occasions, it sure is not in all. Sophisticated Trojans are in many cases infecting through (legitimate) Norwegian websites, that through vulnerabilities has been exploited to host malicious code[39].

Looking more broadly (internationally) for similar research having been conducted in other countries, we found (as mentioned in our introductory chapter) that Checkpoint had conducted a survey on the topic of Social Engineering[8] where 853 IT-professionals participated.

There exist some surveys considering *Phishing*, which are one of those techniques used by Social Engineerings to reach their goals, but we want to gather a *broader* view on the popularity of Social Engineering attacks, as well as limiting our scope to Norway. For doing so we require a method that focuses on contemporary events, as we are interested in finding out how popular Social Engineering is as an vector of attack in Norway *today*. Using either experiments or case studies would not be that beneficial to answer this particular research question, because in order to find out the popularity we need to retrieve data from as many objects (organizations) as possible. This would take to much time for us to be feasible in practise.

Using a survey would seem as the most appropriate method to gather such empirical data. We could have interviewed many organizations regarding their experience with Social Engineering, but again, using the same arguments as with experiments and case studies, it would consume

to many hours to be justifiable. Using a Questionnaire for this purpose is very likely the method of approach of which give us the best cost/benefit. We still however, have the option of asking Qualitative or Quantitative questions, or a combination of both. We will discuss this further in our next chapter, *Design of Questionnaire* (4).

When developing our Questionnaire, it should conform to two demands as said by Dag Ingvar Jacobsen in his (Norwegian) book "How to conduct surveys"[41]:

1. The Empirical data must be valid
2. The Empirical data must be reliable

He elaborate further that the first demand consider that we actually measure what we want to measure, that what we have measures is conceived as relevant, and that which we measure at a few objects, can in some way be generalized. His second demand consider that we have actually measured what we *think* we have measured, that our conclusion is valid in terms of the empirical data. Further it means that the data we have collected is actually representative enough to be able to say something about something. Lastly, the Questionnaire must be conducted in such a way that one can trust the results of it.

When designing our Questionnaire it is important keeping in mind the above. In our chapter presenting the results from our Questionnaire (5), we also discuss these bulletins, against our work.

3.2 What are the common and effective Social Engineering methods today?

We concluded2.4 in our prior chapter about what we know about Social Engineering, that we need to gather up-to-date data to answer this research question. (Finding out what attacks are common *today*).

For finding this out we also here require a method focusing on contemporary events. This should in accordance to the mentioned table1 rule out the research method *History*. We must however remember that we likely need to gather knowledge about earlier attacks beforehand, to find out if some of those are still applicable. We therefore need to review literature and earlier research, before looking for contemporary data.

In the next column we are to differentiate on what *form* the research question has. As the form of this question uses *what*, the table rules out both *Case Study* and *Experiments*, leaving only *Survey* and *Archival Analysis* behind. They could both be suitable to answer a typical what-question. However, as mentioned in our prior chapter (2), roughly 1% of incidents are reported. We therefore likely face high under-reporting in Social Engineering, as organizations do not enjoy showing they are vulnerable.

Chances are therefore slim that we can benefit from looking at archival records, because few businesses are unlikely to have been contributed to such, and if some have, they will not be representative enough to answer our research question. This because we also want to get (anonymous) answers from those usually not reporting as well. We therefore end up by *Survey* being the appropriate method to answer this research-question.

Further we can use both interviews and questionnaires to retrieve data, but as priorly stated, limitation of time makes interviews a less viable alternative. We should therefore use our Questionnaire to address this research question as well. Though, as briefly mentioned before, we have conducted some *preliminary* interviews with professionals experienced with Social Engineering and Security Awareness. This has been beneficial into giving input to the design of the Questionnaire.

3.3 How can an Organization defend itself against Social Engineering?

If this research question require a method that focus on contemporary events can be discussed. It would seem appropriate at first sight, as there is a rather tight connection between this research question and our third one (What are the common and effective Social Engineering methods today?) - we need to find defenses for those attacks found to be common, which may be fairly new ones.

As mentioned it is important retrieving up-to-date data, and in such a case it could be interesting taking benefit of an experiment, case study or survey, or all above, as these methods are considered to yield contemporary data. However, as the nature of this research question is rather wide and open (it ask generally, *how can?*), we need to be open to all incoming data, both known and unknown. This therefore make experiments and case studies not that viable approaches to use, as they are best at studying a particular phenomenon. If our research question had been: *Is identification by codewords*[2] *a viable approach for organizations to defend themselves against Social Engineering?*, experiments and case studies would be much more applicable, because one can then set up a scenario surrounding if this indeed is the case. However, what we basically want, which of course is to ambiguous to be feasible pulling of in practise, but which should be something to strive for, is to gather *all* known (and unknown!) relevant best-practises for defending against Social Engineering - *from the whole world*.

As said, this is impossible to do, but the challenge still remains: we need to gather defense mechanisms that are considered effective, of which at the same time are up-to-date.

Though as mentioned earlier, several authors have in their books also included their thoughts on how to defend oneself against Social Engineering. There also exist several articles written that addresses the same topic. Studying this literature should therefore be one step towards answering this research question. Further, in the discussion of our research question about the popularity of Social Engineering (3.1), we came to the conclusion that using a Questionnaire would be a viable approach to gather the status of today.

Using the same Questionnaire, we could extend it to not only ask questions about the experi-

[2]Identification by codewords is basically that both parties of a relation has a list of numbered codewords priorly agreed upon. When one of the parties contact the other, they need to present a codeword chosen by the opposed party, so to show that they really are who they say they are. The security hole in such a scenario, consider if an adversary get a hold of the list of codewords, or part of it.

ence the various organizations have with Social Engineering, but also what *they do* to defend themselves. This way we get up-to-date data of what organizations today are actually using in regard to methods for defending against Social Engineering.

Such a qualitative approach over a Questionnaire may not however, despite having good intentions, thoroughly explain *how* they are actually defending themselves. They may say a few words of what they are doing, but much more than this we should not expect. And do also note, that just because an organization use a particular method of defense, does not automatically mean that the particular approach is an effective one. If combining the study of literature, with qualitative questions in a Questionnaire, and further *interviewing* professionals within information security that works closely with security awareness/Social Engineering, we could gather the essence from the three sources and then hopefully be able to come to some methods that are considered to be efficient.

3.4 Summary of methods used for this Thesis

Below is a summary of the methods we chose to answer our research-questions:

- Research question 2 - How popular is Social Engineering as an vector of attack in Norway?
  - Questionnaire aimed towards Norwegian Organizations
- Research question 3 - What are the common and effective Social Engineering methods today?
  - Review of earlier research and literature
  - Questionnaire aimed towards Norwegian Organizations
- Research question 4 - How can an organization defend itself against Social Engineering?
  - Review of earlier research and literature
  - Questionnaire aimed towards Norwegian Organizations

3.5 Ethical and legal considerations when conducting Surveys

Dag Ingvar Jacobsen, in his book *How to conduct Surveys*[41] writes (quoting, but translated to English): *The basis of the research ethics in Norway today is surrounding three ground principles tied to the relationship between the scientist and the studied:*

- Informed Consent
- The right of privacy
- The right to be properly quoted

This is further retrieved from the Norwegian website about research; www.etikkom.no[42]

3.5.1 Informed Consent

Informed Consent is divided into the following categories:

- Competence - the respondent must be competent enough to see advantages and disadvantages about participating in the study
- Voluntary - Must be able to decide for oneself if one want to participate or not, without no pressure/interfering from others
- Full Information - Information about the intention of the study and how it will be used
- Understanding - That the respondent *understands* what he/she is participating in

It is not always feasible complying to all requirements, but one should always critically view ones study up against these criteria.

3.5.2 The right of privacy

It is important that the scientist critically assess

- How sensitive the information that will be gathered is
- How private the information that will be gathered is
- How likely it is that one could identify the respondent based on answers
  Needless to say, Questionnaires, interviews, and similar should of course be treated anonymously.

3.5.3 The right to be properly quoted

One should not present answers given by the studied out-of-context, in such a way that it does not represent what the studied meant by the answer.

3.5.4 Social Engineering Experiment / Case Study

Opportunities to perform Social Engineering tests, or certain experiments towards Organisations, could have surfaced. Taking into account our limited experience with this sort of testing, as well as the ethical issues surfacing when tricking/manipulating users, we decided early on not to commit to such activities.

We did however consider the possibility of conducting a Case Study, where the goal was to investigate how "easy" it would be to commit a successful Social Engineering attack. This would basically be done by asking participants various questions about Social Engineering, ex. "If someone arrived at your reception and said they had an appointment with someone in your organization, but you could not find any documented information of this - would you let them in?"

The idea with these questions were to "map", and at the same time, *educate* the participants about their insights of Social Engineering attacks. We did however here as well arrive at the conclusion of *not* conducting such a Case Study because of the limitation of time, as well as the following two issues/reasons:

- If people know they are currently being tested about how easily they are tricked, they sure will strive to not be tricked - consequently resulting in non-valid answers. In a real-life scenario, as opposed to a fixed and set environment with nothing else to focus on than answering questions, participants would very likely react/answer in a different manner, as

there is usually a constant pressure on performing well. One is therefore more likely to do fast and spontaneous decisions, which a Social Engineer take advantage off.

- To achieve valid results we would therefore need to perform a Case Study (or in practise a Social Engineering test) *without* the participants knowing, which instantly gives us Ethical problems.

4 Design of Questionnaire

The purpose of our Questionnaire is to find out how popular Social Engineering is as an attack-vector in Norway, what attacks are common, as well as what defense mechanisms organizations have implemented to counter Social Engineering.
We found it suitable focusing on organizations, rather than on individuals, being it is potentially much more disastrous attacking an organization. Do note however, that SE-attacks target individuals in order to get a foothold within the organization.

As Gjøvik University College had an agreement with Questback[1], letting students use Questback free of charge for a period of 180 days, we chose this tool as the platform for our Questionnaire. We did not compare Questback with other similar tools, because it seemed to give us sufficient functionality and customization.

Using an electronic questionnaire facilitates a lower threshold of answering, as one can do it through ones computer and do not need to bother with how/when to send it back. It also make it convenient gathering results, as answers already have been imported into an electronic environment. It is however important knowing how to analyse answers *before* sending out the questionnaire, as it may reflect upon the questions how one choose to analyse the data they result in.

4.1 Quantitative vs Qualitative

Basically, Quantitative methods will give us general understanding of something, while at the same time *not* giving in-depth understanding. Using a Quantitative approach makes it easier to see trends as one can compare numbers instead of text. Qualitative methods will give us more in-depth understanding, but will make it harder to analyse and compare answers.

Following a table comparing the two, retrieved from the Norwegian book "How to conduct surveys", written by Dag Ingvar Jacobsen[41]

[1] Questback provides electronic questionnaires

	Quantitative methods	Qualitative methods
Should be used when we have:	good knowledge about what we are to study	little knowledge about what we are to study
- when we are going to:	test theories and hypothesises	establish new theories and hypothesises
- when we have:	a wish of generalising (know something about many subjects)	a wish of not generalising (know much about few subjects)
- when we want:	to find out how often a phenomenon happens	to find out the contents of a phenomenon
Pros	Many subjects	depth and understanding of details
	Possibility of generalising from a sample of the population with high degree of certainty	Comprehensive understanding of a phenomenon/situation/individual
	Relatively low costs	Flexible data collection
Cons	Superficial information	Over-complex and to detailed information
	Rigidity in the data collection	rigidity in the data collection
	We impose people particular opinions through standardized questions and answers	High costs, particularly in analysis-phase
	Analytical distance can provide low understanding	Proximity to the respondent can compromise the ability to analyse correctly
		Too much flexibility can lead to the survey never being completed

Table 2: Quantitative VS Qualitative Methods

When investigating how popular Social Engineering is in Norway it is important for us to easily compare the various answers we get, so we increase the likelihood of drawing valid conclusions about the current status in Norway. At the same time however, it is also interesting gathering elaborated information from the participants, if they say that they have experienced SE-attacks. In such a scenario we are interested in more thorough explanation of what kind of attacks this really are, and how they came to happen.

As we want to find out how popular Social Engineering is, we need to ask questions, and give alternatives, in such a way that we can actually measure the frequency of attacks. As stated in Jacobsen's book, when having few possible answers (and one know them) one should use static alternatives. Benefiting from Jacobsen's table 2 above, we see that using a quantitative approach is appropriate for this as we based on literature reviews and preliminary interviews have gathered good knowledge regarding what attacks that can take place, and therefore can ask specific question regarding it.

However, regarding defenses, we do expect them being much more unique and tailored for each organization, to not say they likely will vary quite a bit in regard to what the various organizations have chosen to implement. If asking a set amount of question, asking if the organization are using a specific kind of defense, we stand upon a great amount of questions, to not say that we might deny a respondent telling of his mechanisms if it is not present among our alternatives. (This could have been countered using an "other"-alternative combined with a text-field though)

We decided to use a full qualitative approach in this regard, were we asked what mechanisms were implemented and in which the respondent could answer what they wanted.

However, in hindsight, we would likely have been better off asking something similar to *what defense mechanisms of the following have you implemented?*, for thereafter presenting every kind of mechanisms in a *multiple-choice matrix*, making it possible for respondents choosing several alternatives. We could further have added the option of "other" if respondents felt they could contribute with more mechanisms. If having used this approach it would have been more manageable analyzing the results and drawing conclusion upon the respondent-pool, as well as making it easier for the respondent, not needing to think/remember through all possible mechanisms that could be relevant.

In our Questionnaire we combined the use of Quantitative and Qualitative methods within the same Questionnaire. We started with Quantitative questions, but added causal-related Questions that would only be asked if they chose a specific answers. They would then be given the option of elaborating on the option they chose, if wanting to.

4.1.1 No Comment

We acknowledged from the start; doing research on Social Engineering could result in "paradoxical" situations. As we priorly stated, Social Engineering is more or less about manipulating people into releasing sensitive information or services. Giving out information regarding what attacks one experience, and even about what attacks that has been successful, for not to say what defense mechanisms one have in place, is not be hard to argue for potentially being sensitive information, or at least categorized as internal information. Nevertheless we asked these questions in our Questionnaire. Using the Survey-tool Questback, it should give sufficient anonymity. We added the option of answering "No Comment" in case the respondent felt uncomfortable answering a specific question - we considered it to be more beneficial receiving *some* answers, than none. Few respondents did however take the liberty of using this alternative.

4.2 Visual Design of Questionnaire

If one do not take some effort into the making of a logical design of the Questionnaire, one risk to get less accurate results because of misunderstandings, or even respondents dropping out of the Questionnaire before having finished it.

We could use Dropdown alternatives that the respondent click on, for so to get all the alternatives, but in practise this didn't look so *clean* (please find an example below in figure 11). We decided to go for a Multi Matrix10. Besides being more structured, it also gives the respondent a visual aid when answering the questions; when deciding for an answer, one see immediately if that answer looks unreasonable, if putting it in front of a different answer for instance.

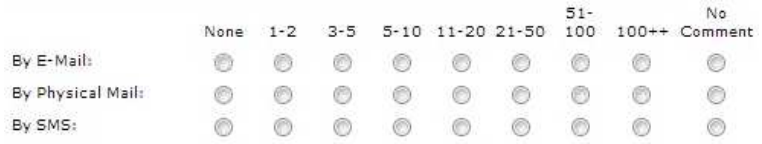

Figure 10: Our approach - using a multi matrix

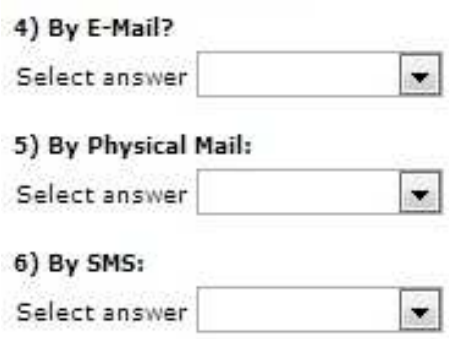

Figure 11: Another approach - using drop-down lists

4.2.1 Five pages, five topics

To make the Questionnaire as clean and structured as possible, we decided to split up each section in the Questionnaire, making one page cover one topic:

- Introduction with general questions
- Attacks
- Successful Attacks
- Defense Mechanisms
- Elaboration

Dividing the Questionnaire up into these parts makes the respondent able to focus and finish one "category" before moving on to the next, as well as giving a sense of progress in the Questionnaire.

The following paragraphs below describes the various sections in the Questionnaire. To see the Questionnaire as it was presented for the respondents, please see the Appendix.

Introduction

On this page we wanted to give an introduction to the Questionnaire, as well as give a definition of Social Engineering, so to increase the likelihood of every respondent answering with the same basis. We also stated the time frame of which we wanted the respondent to consider questions up against (since the 1st of January, 2011).

One often asks the respondent of what industry it belongs to, as this can show interesting results. It could be that the banking-industry discovered more attacks than the construction-industry, for instance. However, as there are many industries to choose from, and we knew that we would get a limited amount of respondents to the Questionnaire, we would likely have arrived at a scenario were only having a few respondents in each industry.

Scientifically speaking we would therefore have a hard time to argument for a certain industry being prone to SE-attacks (because of the lack of respondents in that industry).

Taking into account that it is sometimes a tedious task finding out which option to choose from (when industries are listed), as there is no standard on how to list industries, we arrived at letting the respondents write themselves what industry they belonged to. How specific they wanted to be, if even wanting to answer, they could choose for themselves. Using this alternative makes the respondent use much less time on finding the appropriate option, as well as it gives us the *possibility* to analyse answers given up against industries.

NON-Targeted / Targeted attacks

We had defined seven *channels* for conducting SE-attacks:

- By E-Mail
- By Physical Mail
- By SMS
- By Phone
- By Adversary physically showing up in person
- By using Social Networks, like Facebook
- By surfing on websites

We found it interesting looking into the possible difference on targeted and non-targeted attacks. We therefore asked the same questions two times, one for each. For each channel we asked the frequency in which the organization experienced attacks.

At isc.sans.edu[43], Maarten Van Horenbeeck proposed a graph (figure 12 below) categorizing Social Engineering attacks based upon the potential revenue it may have for an adversary when attacking a victim.

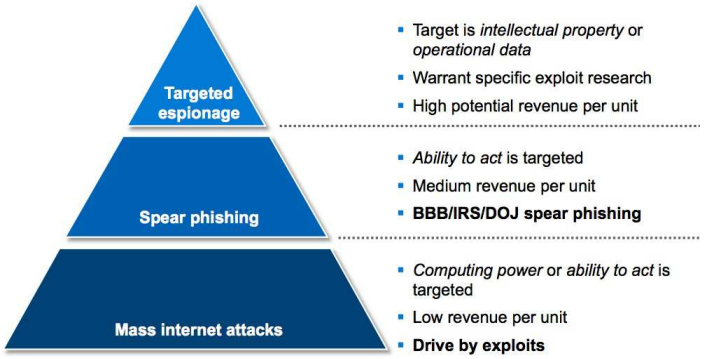

Figure 12: Social Engineering categorised by potential revenue. By Maarten Van Horenbeeck

What is interesting observing from our Questionnaire, is if there is a clear distinction between those attacks considered non-targeted, and those considered targeted, following the principle as Horenbeeck propose in the graph above (12).

Successful attacks

This section follows the same principles as in the prior section, except for asking for *successful* attacks. These answers not only says something about the frequency, but also how able the respondents in question are to detect attacks that have taken place, as well as how big of a security risk SE is in practise.

Defense Mechanisms

In this section we wanted to get an understanding of how prepared organizations are against Social Engineering threats.

Elaborating

In this section we gave respondents the opportunity to elaborate on their quantitative answers given in the section of defense. Most of these questions were causally tied towards the answers priorly given, so if saying "yes" to having defense mechanisms, they would get a question asking for what mechanisms they had. If answering "no" they would get a question asking why they did not have any mechanisms in place. We finished with a question asking about how they conceived the security risk of Social Engineering to be toward their organization.

4.3 Finding Respondents

Gathering respondents may be the hardest part when conducting a survey. Suddenly one is dependent upon people one don't even know. There are several alternatives on how to gather participants. We will now shortly describe the alternatives we chose and why.

Contacting respondents indirectly

In the ever-growing age of the Internet, and all it's Social Media, it has become possible connecting to other people "like you". Take LinkedIN for instance, here one can join various professional groups that persist of people with similar background to oneself, or at least have some of the similar interest.

Using this for our benefit, we decided to post a discussion about our Questionnaire on one of these groups, asking politely the group's members to participate. By doing this we were able to reach several hundreds of Information Security interested people with very little effort. However, not all of these members are likely to have a position where they could *represent* a Company for the purpose of our Questionnaire about Social Engineering, but it gave us some "free" respondents.

It was important though, to some extent, have control of who actually participated in the Survey, so to not get phony answers. We therefore required participants to send us an email stating they wanted to participate, as well as what Company they represented for this purpose. Committing like this has both an advantage, and a disadvantage; Before we actually send out the Questionnaire we are more knowledgeable of how many respondents we actually get, but people could be more reluctant to commit "formally", maybe resulting in less initial respondents.

Contacting respondents directly

One can contact an organization directly by; physically visiting them, phone them, E-mail them, and perhaps even send them a physical letter. These methods require one to contact each and every Company out there, resulting in quite a lot of effort needed. In our case that is actually particularly challenging, because we needed to get in contact with those within an organization that are responsible for Information Security, or someone having enough knowledge and overview, being able to represent the company as a whole in regard to answering questions about Social Engineering. This would generally in practise mean likely the minimum of two "hops" for each organization - first one when talking with the switchboard, and then (if lucky) the responsible person itself. Though it is not always easy being transferred to the *correct* individual.

We did however take benefit of the fact that many people state their current job position on for instance LinkedIN and/or company web pages. Looking for those people having some sort of responsibility for Information Security, we were mostly able to "skip" going through the switchboard, and by other means find contact-details directly to those we needed to speak with. The benefit from this was that we could use off-hours to find contact-information, while use the daytime to actually conduct the phone calls.

An inquiry were be sent out to identified Organisations before an invitation to the questionnaire were sent (in most cases our initial phone call), asking if they would like to participate as well as a short introduction of the Master Thesis. The main reason for doing so was to be polite. However, we are all asked from time to time, either by phone or email, to buy some products and/or answer a survey, very shortly after the whole idea of it has been proposed. Few people

have time *right now* to commit such time, but time in the future is more likely people can commit.

We therefore have two positive effects: More recipients to questionnaires, as well as an idea before the questionnaire was been sent out on how many responses we would get. This was beneficial for us, as we then could have taken precautions to not get caught in a situation with very few respondents and limited time left to get more.

We will now, in our next chapter, present and discuss the results of our Questionnaire.

5 Data analysis - results from Questionnaire

5.1 Introduction of the data analysis

5.1.1 Research Lens

In one of his books; *Qualitative Research from Start to Finish*[44], Robert K. Yin points out what he calls the *Research Lens*; despite wanting and urging to perform a study with a neutral mind, it is impossible reaching total neutrality. One individual could analyse some data and take out some interesting observation, while another individual could analyse the same dataset and come up with a different observation - not necessarily a contradictory observation, but maybe a whole different observation all together. If sitting on the train and looking out the window, one person may find the trees particularly nice, while another find them very annoying, because they are blocking the view of the beautiful ocean behind.

Basically the Research Lens is how each individual would interpret a certain study. For instance, if one are "leaning" in a certain direction before the study has been performed, one may be more likely to favour those facts and evidences that argument for this direction being true, and down-playing those arguments that are against this vision. The author writing this Master Thesis for instance, is convinced that Social Engineering works as an vector of attack. Dedicating enough time towards a certain company, it would very likely result in a successful attack, is his mindset. This is however just the *thought* and *hypothesis* of *this* author, and we should have this in mind when analysing the data so to not colour what we actually observe.

5.1.2 The Hawthorne-effect

As pointed out by Jacobsen in *How to conduct Survey*[41]; at the moment one are conducting any kind of survey, one risk the participants being influenced in some way, possibly leading to less valid answers. This concept is also referred to as the *Hawthorne-effect*. In regard to our Questionnaire, a good example is the last question we asked: *How big of a security risk do you consider Social Engineering to be towards your Organization?*. After having thought through how to answer each of the prior questions, chances are that the risk of Social Engineering, as conceived by the respondent, had changed, compared to when starting on the Questionnaire. It is not possible either confirming or de-confirming this effect for our results, but is something to keep in mind.

5.1.3 Questionnaire

The Questionnaire had in total 52 invitees, whereas 44 answered. This yields an answer-rate of roughly 84,6%, which is fairly good for a questionnaire like this. This is however slightly coloured, as the majority of those invited beforehand had been agreed upon to participate in the Questionnaire. The respondents represent various industries in Norway, of which most were contacted directly by phone.

A typical respondent would be a CSO/CISO[1] of an organization, or others that have an overview of what attacks the organization is experiencing. The Questionnaire went public at the 15th of March, 2013 and was planned being active until the 15th of April (which was expressed to respondents in the beginning of the period).

We did however decide to extend the period in which the Questionnaire was active until the end of April, to gather more respondents. This information was communicated to new respondents, but not "old ones". We did however not deactivate the Questionnaire before the actual formal delivery of the Thesis, as we would rather have some late responses, than not have them at all. Some of those respondents being invited early on, might however have believed that responses after the 15th of April was not being analysed and might therefore have chosen not to respond. Two responses arrived after the end of April - they are included in the datasets.

We now proceed with the actual analysis and presentation of our results.

[1] CSO: Chief Security Officer / CISO: Chief Information Security Officer

5.2 Industry of the Organizations

We asked: *What type of Organization do you represent?*

The respondents answered by writing their industry in a text-field, they could choose how specific they wanted to be.

Depending on the amount of "hits" we got in a certain industry, we might have been able to generalise by saying that a certain industry experience more attacks than others. The industries were however quite spread around in different arenas. The value of an analysis based on industry is therefore rather limited. This was also something that we more or less expected beforehand. One could likely neglected using this question, but still it is somewhat "normal" to include. It could have given valuable results, and we therefore still feel confident having used it. Further we chose to not list up the various answers given to this question, so to limit potential speculation in regard to which organizations participated in the survey.

5.3 Amount of Employees in each Organization

We asked: *How many employees does your Organization consist of? (of which you can represent for the purpose of this Questionnaire)*

Though "randomly" contacted, the amount of employees each organization consisted of is rather evenly spread, with most (93,2%) organizations consisting of more than 50 employees. Further, 43,2% of the organizations consisted of more than 1000 employees. This is interesting, because it essentially means that the total amount of employees represented by this Questionnaire goes beyond 100.000. Please notice the difference in colour of those respondent consisting of more than 1000 employees - for all graphs considering *attacks*, we distinguish between those respondents having more than 1000 employees (always at the bottom of the bar), and those having less (always at the top).

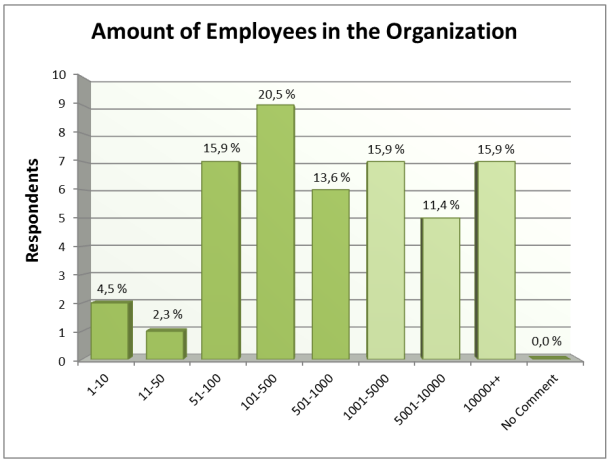

Figure 13: Amount of employees in Organization

5.3.1 Presenting the results

We will now present and discuss the results regarding the various attacks our respondents have experienced. These results may be presented in several ways, but we mainly considered two approaches; we basically asked the same questions four times (How many times have your Organization experienced (...) Social Engineering attacks?: (i) non-targeted, (ii) targeted, (iii) non-targeted and successful, and (iv) targeted and successful.

The obvious is to either compare non-targeted with targeted, or non-targeted with non-targeted that are successful. (Two on each page). Though both approaches are interesting, the last alternative may show greater value, as one may discuss how many of all attacks have been successful; of these 100 attacks, 5 have been successful. Despite the accuracy not being that great, as all alternatives are in intervals, it still gives an indication of the percentage of all attacks being successful.

We could also choose to add *attacks* and *successful attacks* to the *same* graph. Visually however, that might be more confusing than not: Say that we have 100 attacks by email, whereas 11-20 are successful ones. This would result in the 11-20 bar sky-rocketing whereas 100++ hitting rock-bottom, this may make it appear rather inconsistent.

We therefore chose to present two separate graphs. Further however, it is overly important that we remember that a successful Social Engineering attack, in its truest form, *will not* be detected. This would not only have consequences for the validity of the graphs considering successful attacks, but also those considering *all* attacks.

We considered using bubble-charts to show one more dimension of information, using the same space, but the nature of our alternatives (being intervals) make it not that viable for presenting our results in an easy-to-read format. Bubble-charts are very nice when handling data having one-to-one relation between it's components.

The first section, starting at the next page, present those attacks that are considered to be *NON-targeted*, of which afterwards, those attacks considered to be *targeted* will be presented. Further one will find two graphs on every page; the first graph showing *all* attacks, and the second graph showing *successful* attacks. We will discuss each graph separately, before comparing them.

As mentioned on the prior page considering the amount of employees of our respondents, in most graphs we distinguish by respondents having more than 1000 employees, and those having less. This is done by using different colours within the same bars. (Brightest green representing respondents with more than 1000 employees). Please have a look at the graph showing employees (5.3) for a visual representation of the colours. The colours should also be highly apparent if printing out this document in grey-scale.

5.4 NON-targeted Social Engineering attacks

We asked: *How many times have your Organization experienced (Successful,) NON-targeted Social Engineering attacks?*

5.4.1 All attacks By E-Mail:

We see that the use of E-mail are very popular as a channel for conducting Social Engineering attacks. Over 50% of the respondents said they had experienced this over 100 times. Almost 85% stated they have experienced it one or more times, while the rest were unsure about the amount.

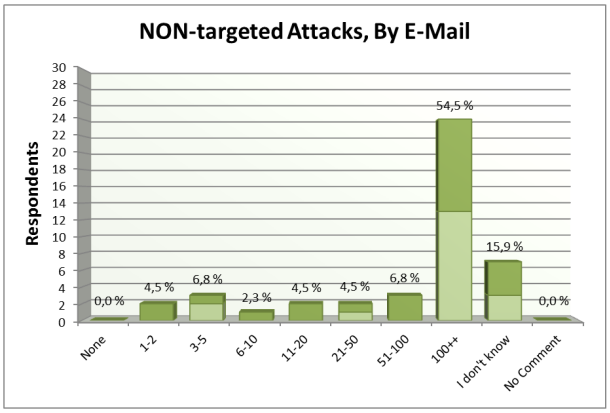

Figure 14: Non-targeted attacks By E-Mail

5.4.2 Successful attacks By E-Mail:

36,4% said they had experienced a successful attack by E-Mail. Further 25% stated they were unsure of the amount, as well as roughly 34% saying they had experienced no successful attacks.

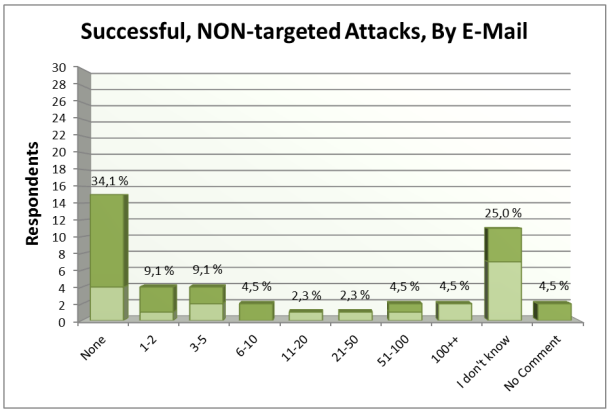

Figure 15: Successful, Non-targeted attacks By E-Mail

NON-targeted attacks are very cost-effective, because one can basically make one template/edition and send it to many recipients.

5.4.3 All attacks By Physical Mail:

Attacks by physical mail do not appear to be that popular. 18,2% of the respondent stated they had experienced this. Some respondents further elaborated that they had received "fake" invoices, in which they were urged to pay by the sender. Though there in larger organizations not always exist a clear visible line between those having ordered a product or service, and those paying the bills, the consequences of such an "attack" is rather limited.

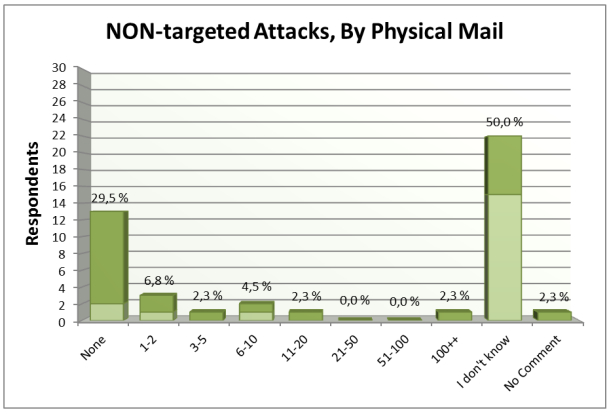

Figure 16: Non-targeted attacks By Physical Mail

5.4.4 Successful attacks By Physical Mail:

A user receiving physical mail have quite limited strings to play on: An "ordinary" user may not have the clearance to issue payments on behalf on the company for instance. These sort of attacks is therefore likely needed to pass through various "chokepoints" (CFO, etc.). This further means that training these "chokepoints" may be an efficient approach to prevent such attacks from being successful.

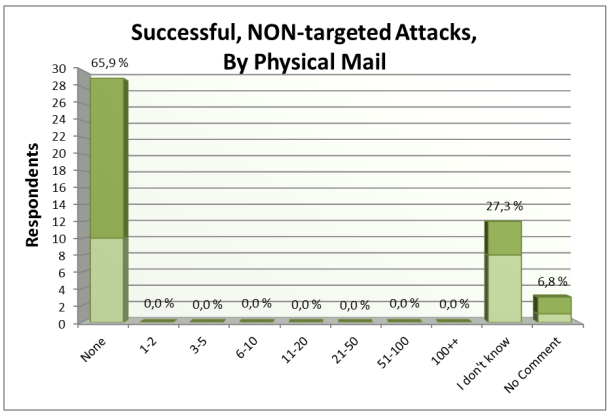

Figure 17: Successful, Non-targeted attacks By Physical Mail

We consider it not surprising that none reported successful attacks on this channel.

5.4.5 All attacks By SMS:

Available services makes it possible sending SMS-messages which appear to be from your bank, the police or similar. Typically one is manipulated into believing that urgent attention is needed by clicking on a certain link. For instance downloading a new update to one's smartphone. The link is of course malicious. Almost 23% say they have seen attacks through SMS. Also this graph, as the one about physical mails, show that almost 50% are not sure of the extend of attacks happening.

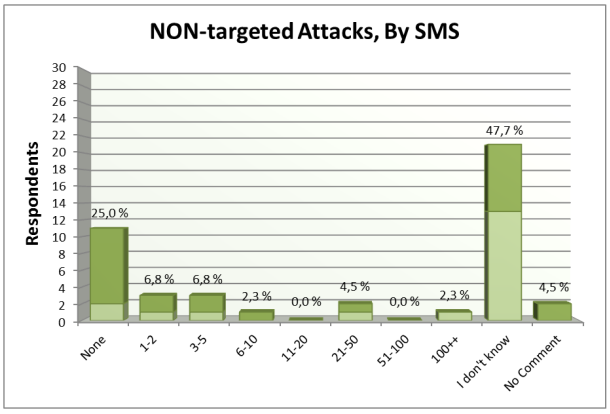

Figure 18: Non-targeted attacks By SMS

5.4.6 Successful attacks By SMS:

59% state they have had no successful attacks.

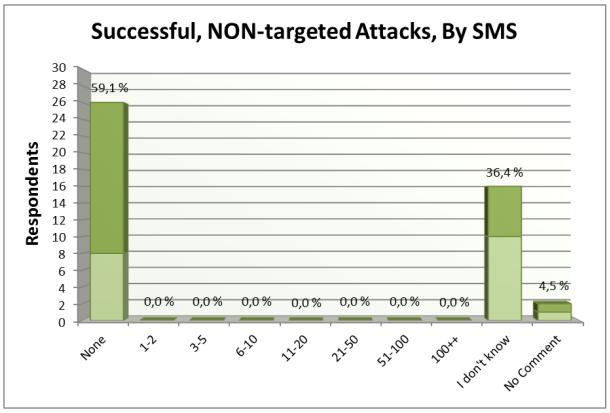

Figure 19: Successful, Non-targeted attacks By SMS

5.4.7 All attacks By Phone:

38,6% say they have experienced attacks by phone. Some respondents mentioned "Microsoft helpdesk" calling, explaining that the reason for your computer being slow (which computer do not appear to be slow sometimes? - The Barnum effect[45][2]) is because of malicious activity. They of course want to help you. It results in the download of malicious software.

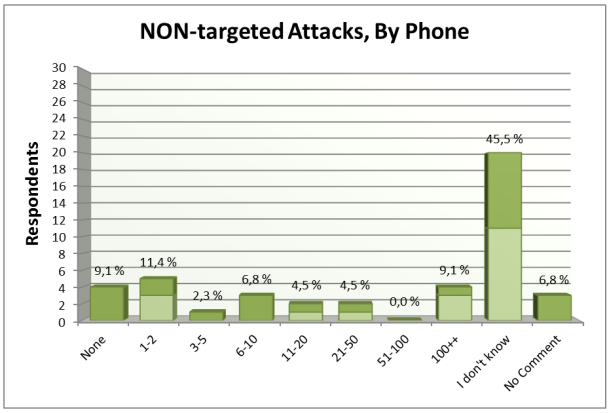

Figure 20: Non-targeted attacks By Phone

5.4.8 Successful attacks By Phone:

Roughly 9% state they have experienced successful attacks by phone.

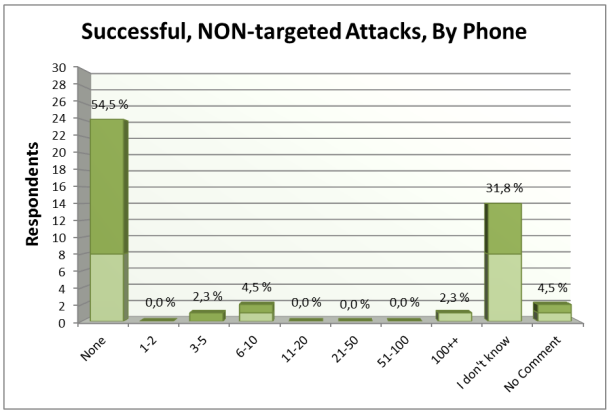

Figure 21: Successful, Non-targeted attacks By Phone

[2]The Barnum effect, as mentioned by David Lacey in *Managing the Human Factor in Information Security*[45], is *a generalized character assessment that can be readily accepted by most people as a personalized one*. Further he says: *It explains, for example, why highly generalized horoscopes in newspapers are commonly perceived as being accurate personal predictions.*

5.4.9 All attacks By Adversary showing up in person:

Though being one of the most risky ways of conducting a Social Engineering attack (showing one's face and voice), 9,1% said they had experienced this type of attack. Three of those organizations having experienced this consist of more than 1000 employees.

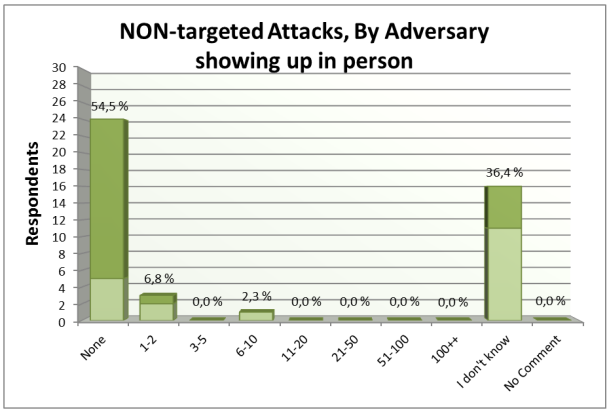

Figure 22: Non-targeted attacks By Adversary showing up in person

5.4.10 Successful attacks By Adversary showing up in person:

4,5% stated they have experienced a successful attack by a person showing him/her-self physically. Both (4,5% = 2) of which are large organizations.

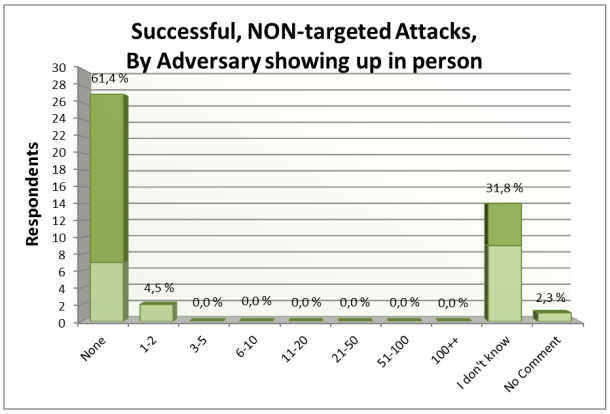

Figure 23: Successful, Non-targeted attacks By Adversary showing up in person

5.4.11 All attacks By using Social Networks, like Facebook:

Almost 23% said they had experienced attacks through Social Networks. An example could be Skype; someone trying to add you saying something like "I saw that you were in my neighbourhood and thought that I should say hi". If accepting the invitation, one will likely be provided a malicious URL. Another example is were someone add you on Facebook, that one *think* one know. The adversary now have access to a vast amount of information, not only about oneself, but also about one's network.

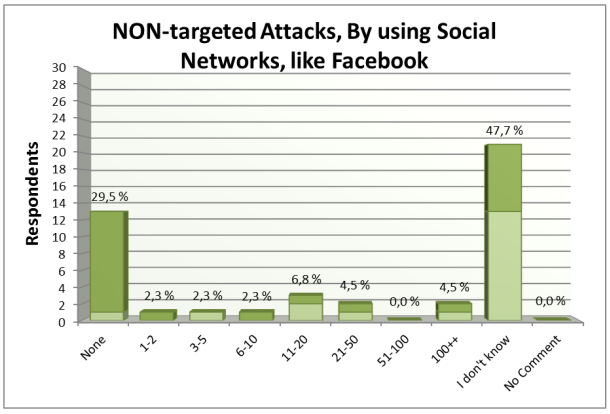

Figure 24: Non-targeted attacks By using Social Networks, like Facebook

5.4.12 Successful attacks By using Social Networks, like Facebook:

11,4% experienced successful attacks through this channel.

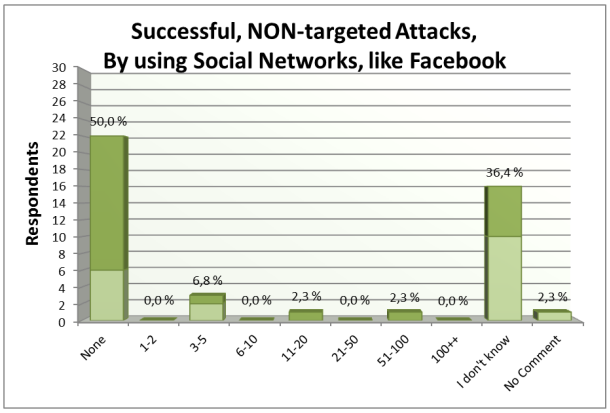

Figure 25: Successful, Non-targeted attacks By using Social Networks, like Facebook

5.4.13 All attacks By surfing on websites

Roughly 50% said they have experienced attacks through surfing on the Internet. This channel is the one that the large organizations has been least unsure about, in regard to non-targeted attacks.

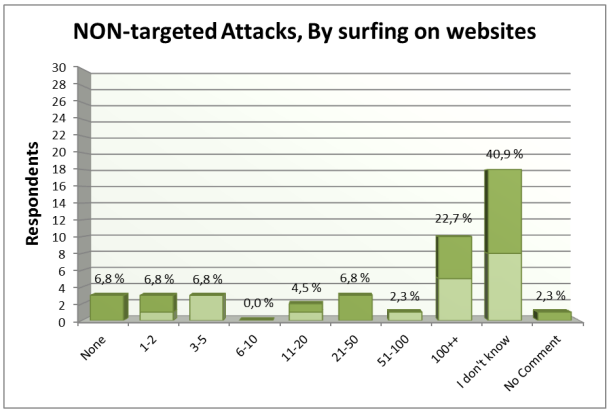

Figure 26: Non-targeted attacks By surfing on websites

5.4.14 Successful attacks By surfing on websites

29,5% said they have experienced successful attacks through navigation on the Internet. Giving away sensitive information (because of phishing), or compromise of one's computer is likely to be the consequence of such an attack.

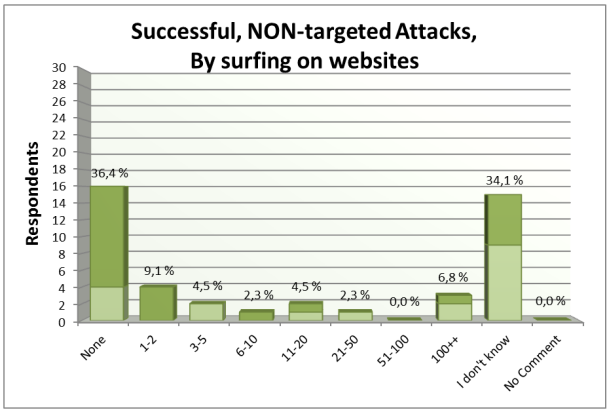

Figure 27: Successful, Non-targeted attacks By surfing on websites

5.5 Targeted Social Engineering attacks

We asked: *How many times have your Organization experienced (Successful,) TARGETED Social Engineering attacks?*

5.5.1 All attacks By E-Mail:

Roughly 43% state they have experienced E-Mail attacks that has been targeted/tailored towards the recipient. It was mentioned that several were targeted towards management-roles in the organization.

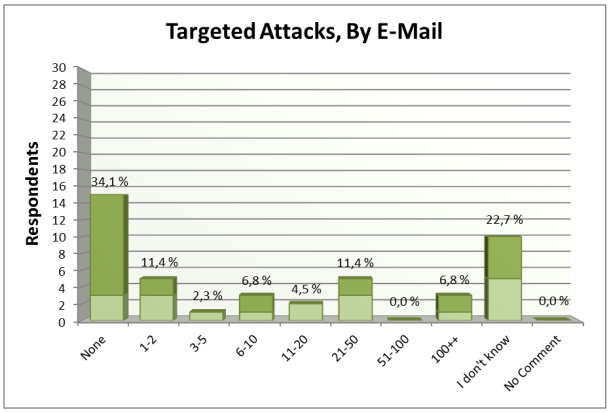

Figure 28: Targeted attacks By E-Mail

5.5.2 Successful attacks By E-Mail:

Roughly 16% said they have experienced successful attacks by targeted E-Mails. Quite evenly distributed between those organizations with more than 1000 employees, and those with less.

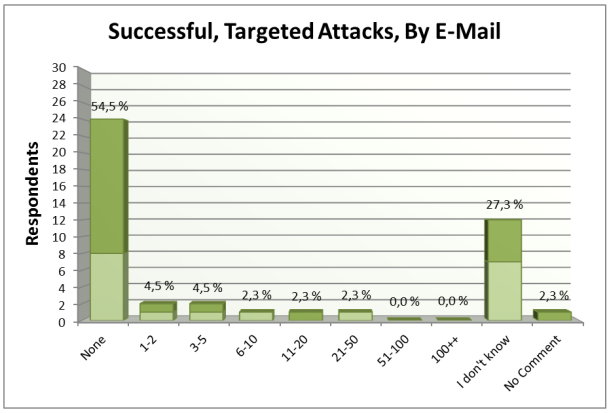

Figure 29: Successful, Targeted attacks By E-Mail

5.5.3 All attacks By Physical Mail:

20,5% said they have experienced physical mails that were considered targeted/tailored towards the organization.

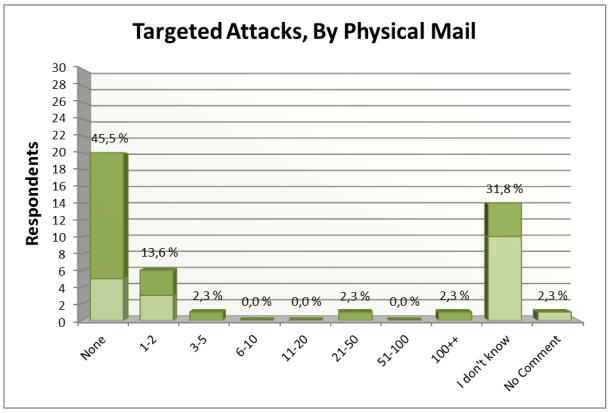

Figure 30: Targeted attacks By Physical Mail

5.5.4 Successful attacks By Physical Mail:

Most organization stated they had no knowledge of successful attacks through this channel. The rest are unsure if they have had any successful attacks, or did not want to say.

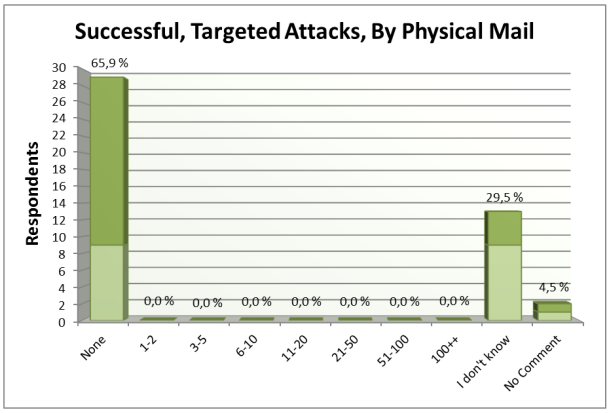

Figure 31: Successful, Targeted attacks By Physical Mail

5.5.5 All attacks By SMS:

Only 6,8% said they had received targeted SMS's. This is actually a bit surprising. We expected a higher frequency of attacks through this channel. However, targeted and successful attacks are more likely to go undetected, resulting in no reporting of it.

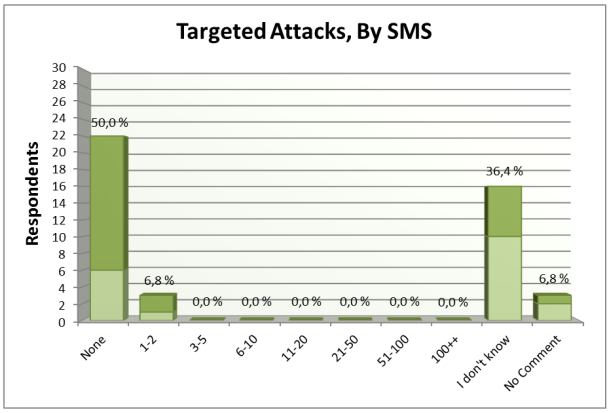

Figure 32: Targeted attacks By SMS

5.5.6 Successful attacks By SMS:

Most organization have not experienced successful attacks through targeted SMS's. The rest are unsure if they have had any successful attacks, or did not want to say.

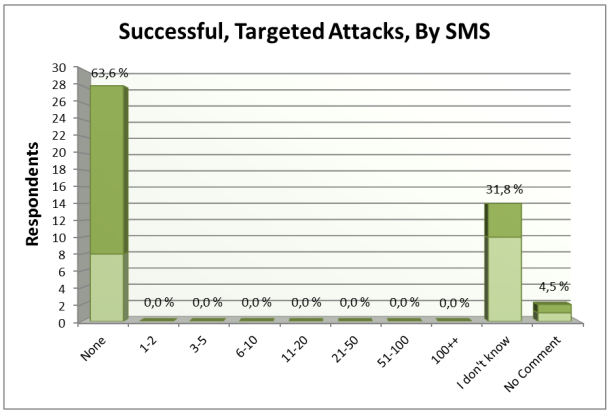

Figure 33: Successful, Targeted attacks By SMS

5.5.7 All attacks By Phone:

27,4% said they have experienced phone calls targeted towards the organization. Two large organizations says they have experienced this with very high frequency. This are interesting numbers.

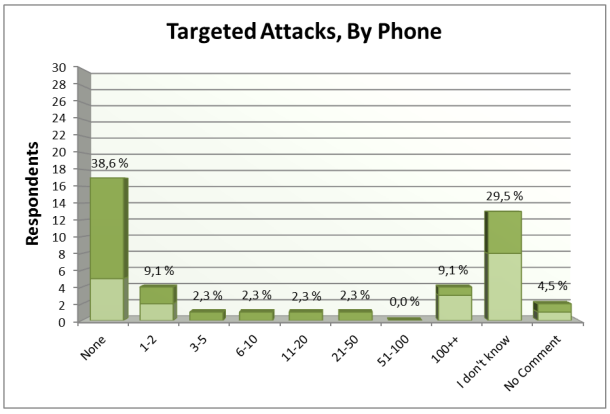

Figure 34: Targeted attacks By Phone

5.5.8 Successful attacks By Phone:

Roughly 9% say say they have experienced targeted phone calls being successful. One large organization state they have experienced a lot of this.

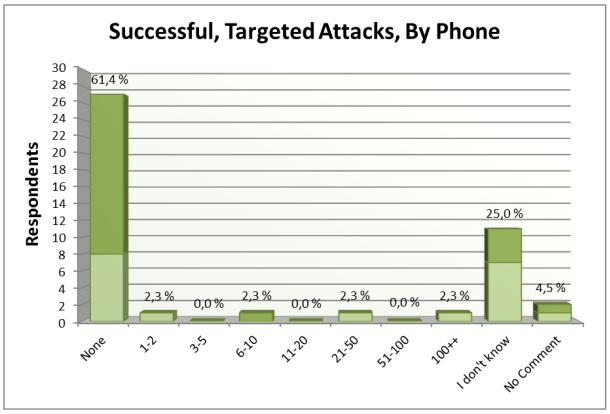

Figure 35: Successful, Targeted attacks By Phone

5.5.9 All attacks By Adversary showing up in person:

Only 4,6% state they have experienced targeted attacks where a person have shown up physically

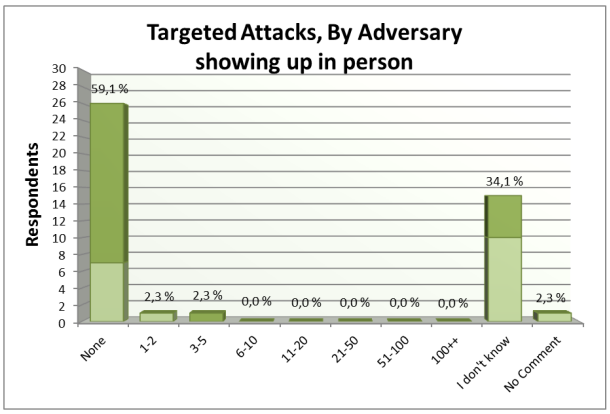

Figure 36: Targeted attacks By Adversary showing up in person

5.5.10 Successful attacks By Adversary showing up in person:

All organization that have experienced a targeted attack like this have also experienced some of them being successful.

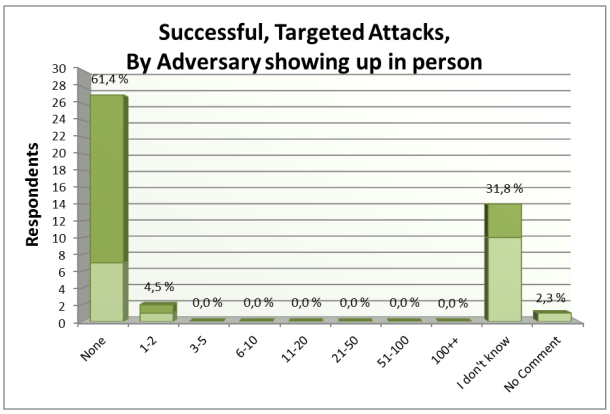

Figure 37: Successful, Targeted attacks By Adversary showing up in person

5.5.11 All attacks By using Social Networks, like Facebook:

11,4% have seen targeted attacks through Social Networks.

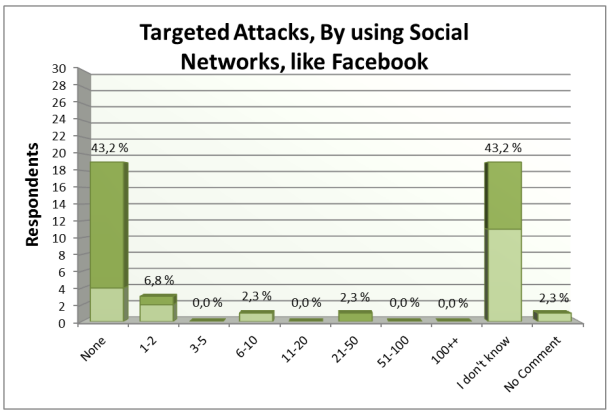

Figure 38: Targeted attacks By using Social Networks, like Facebook

5.5.12 Successful attacks By using Social Networks, like Facebook:

No organizations says they have experienced successful targeted attacks through Social Networks.

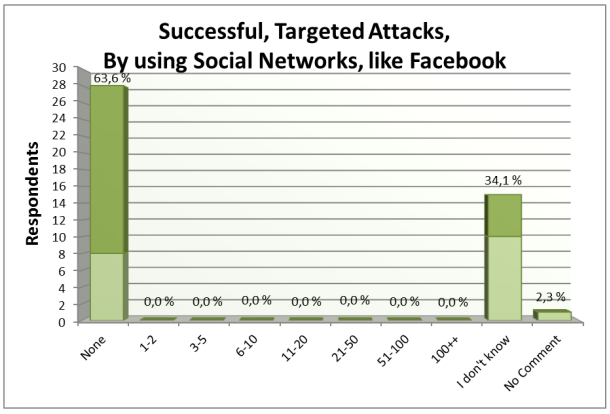

Figure 39: Successful, Targeted attacks By using Social Networks, like Facebook

5.5.13 All attacks By surfing on websites

Rougly 16% have experienced targeted attacks when surfing on the Internet.

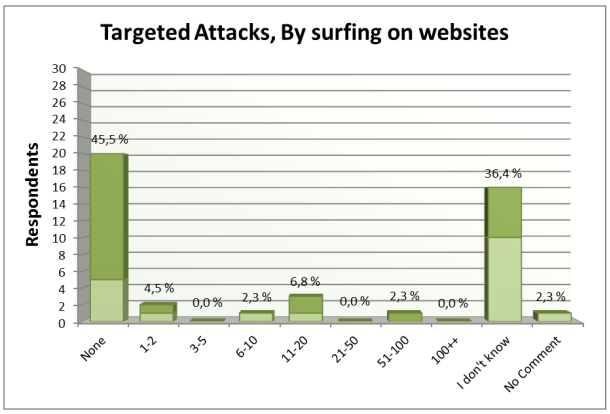

Figure 40: Targeted attacks By surfing on websites

It was mentioned by a respondent that sensors and security monitoring partners often reported addresses associated with known APT groups had accessed the company's website in search of information, then mostly about executives. This may be considered as reconnaissance before launching a real attack.

5.5.14 Successful attacks By surfing on websites

Roughly 9% have experienced successful targeted attacks by surfing on the Internet.

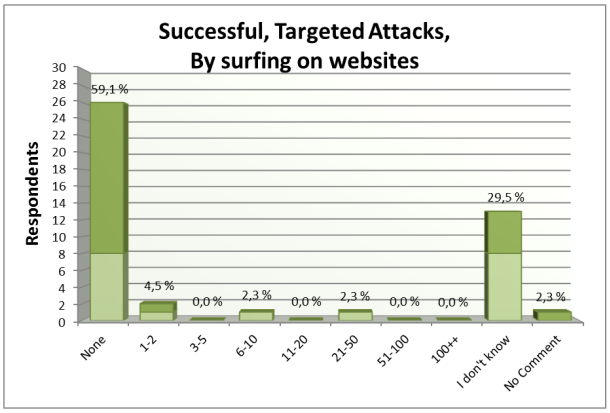

Figure 41: Successful, Targeted attacks By surfing on websites

In February 2013, Digi published an article titled *Search more dangerous than porn*[39]: The article discussed Cisco's yearly security-report which states that it is not the suspicious sites (porn,gambling,filesharing, etc.) that necessarily compromise ones computer any more, but legitimate sites through for instance commercial banners. This results in a new *era* of attacks because where one before could rely on scepticism towards a website, one now have to purely

rely on technical defenses when navigating on the Internet. Cisco state that web advertisements are 182 times more likely to spread malicious code, than websites with adultery material. What this means from an Social Engineering perspective, is that one are not able rely on awareness in that extent.

5.6 Economic losses due to Social Engineering attacks

We asked: *If Successful attacks, what do you estimate your economic losses to be because of it? (In NOK)*

In hindsight, this question should have had one more alternative; *No successful attacks*, so that one could distinguish between those respondents that actually have no known successful attacks, and those that have had, but considered no economic loss to take place because of it. One respondent mentioned that limited economic loss existed, except for the time it took to for instance re-tank client-machines being compromised by malware, as a result of diverse Social Engineering attacks. This could be considered *indirect* economic losses.

Food for thought:

> Though not intended to investigate with this question, we figured afterwards the Questionnaire was published, that the first alternative beginning on *1 NOK*, *likely could* have been chosen by *all* respondents (instead of those choosing *None*), regardless of the consequences of an attack. The reason for this is simple; at the moment one have received a phishing e-mail and started to read it, one have committed time and energy to actually do so. If it only took as short as 15 seconds to come to the conclusion to regard the e-email as fake, in terms of lost man-hours (seconds), that time would very likely be worth *at least* 1 NOK. Installing mail-washers and similar may therefore be one efficient approach for preventing lost man-hours due to reading irrelevant E-Mails.

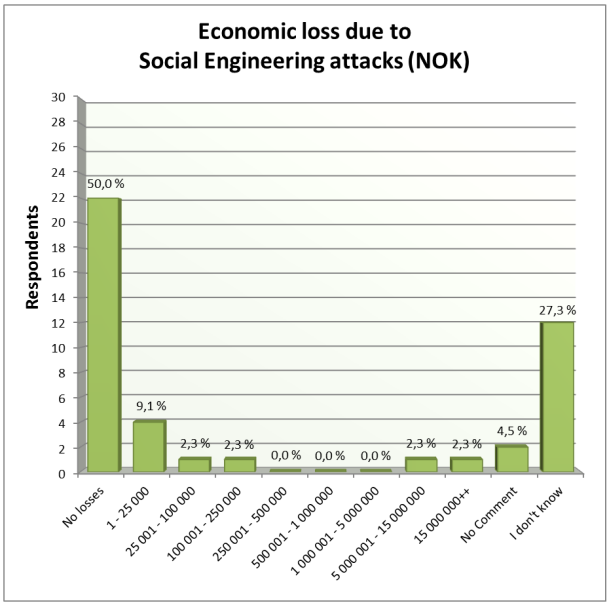

Figure 42: Economic losses due to successful attacks

Half of the organizations said they have experienced no loss due to Social Engineering attacks. It was pointed out that it is not always easy tying an event happening up against a certain economic loss, as losses may not be materialized until years after the event. Examples of this can be an attack towards a company getting publicity from the Media. The company's goodwill may

decrease, resulting in either lost customers/clients in the upcoming future, or lessened arrival of new ones.

18,3% state they have experienced economic loss due to SE-attacks, whereas roughly half of them have had limited losses under 25 000NOK.

What is very interesting with these numbers, are that they seem to show, that the losses due to Social Engineering are either very low/none-existing, or the losses are major, in terms of millions of NOK. The numbers ultimately show how large the consequences of Social Engineering really can be.

When looking at such numbers, one are likely facing loss of trade-secrets, patent-pending products, or other information/items that are very valuable.

To limit speculation on what organizations participated in the survey, we chose to *not* distinguish by respondents in regard to amount of employees in this graph.

5.7 Defense Mechanisms

5.7.1 Do you currently have Defense Mechanisms in place to counter Social Engineering

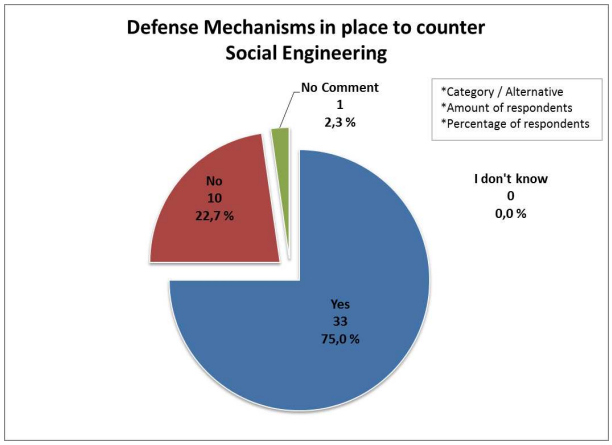

Figure 43: Defense Mechanisms implemented to counter Social Engineering

It is good to see that the Majority of the organizations (75%) have mechanisms in place to counter Social Engineering. For those answering yes/no we asked more specific about *what* mechanisms they had, or *why* they had no mechanisms. 16 respondents mentioned in some way awareness as a defense mechanism. A summary of the answers are provided below.

Short elaboration for those having answered *YES*

We asked: *Can you elaborate on what Defense Mechanisms you have in place to counter Social Engineering? (Detection/Prevention/Correction)*

Below is a summarizing of defense mechanisms the organizations have implemented against Social Engineering. Though the line between the two may not always be apparent, we divide them into *technically oriented* and *not technically oriented* defense mechanisms: (please note that there is not necessarily a one-to-one relation between a bulletin and a respondent, many have been integrated into one another.

Technically oriented defense mechanisms

- Antivirus, firewall, web filters
- E-mail traps (real attack using public employee adresses from e.g. LinkedIN and other social networks)
- No ordinary users are allowed to install software
- Spam-filters
- E-Mail filter
- Network and system monitoring
- Sandboxing techniques on incoming e-mail
- Web-based proxy

- IPS and anti-bot software
- Patching of all systems on a monthly basis
- Limitations in systems, event logging, security monitoring
- Email scanner that warns if links do not lead to the same page as is displayed
- Web content filtering preventing access to landing pages

Not technically oriented defense mechanisms

- Education and awareness training for internal employees, hired personnel, security guards (physical access) and vendors
- General awareness according to our security policy
- Security culture training
- Information campaigns on local Intranet and external websites about phishing
- Information campaigns for customers and employees
- Training of all new employees
- Training of switch board operator and key personnel
- Targeted awareness campaigns for high risk targets
- Employees are challenged to keep themselves up-to-date, perform internal workshops and lectures surrounding security
- Examples of attacks
- Cooperation with security vendors, take down sites
- Cooperation with other businesses in same field
- Incident response procedures
- Identification by our customers by phone, access control (badges etc.)
- Callback and ID checks
- Routines for identifying company personnel prior to giving access to company resources

Short elaboration for those having answered *NO*

We asked: *Can you say anything about -why- you have no Defense Mechanisms in place to counter Social Engineering?*

Below is a summarizing of why not all organizations had implemented defenses against Social Engineering:

- Not an issue in the risk assessment
- Little focus on Social Engineering
- Not having available resources to prioritise it
- Haven't been a priority
- Own "built-in" defense mechanism (Scepticism)
- No mechanisms targeted directly towards Social Engineering, but on security awareness and security culture that automatically also covers Social Engineering

5.7.2 Are you planning on implementing (more) Defense Mechanisms to counter Social Engineering attacks?

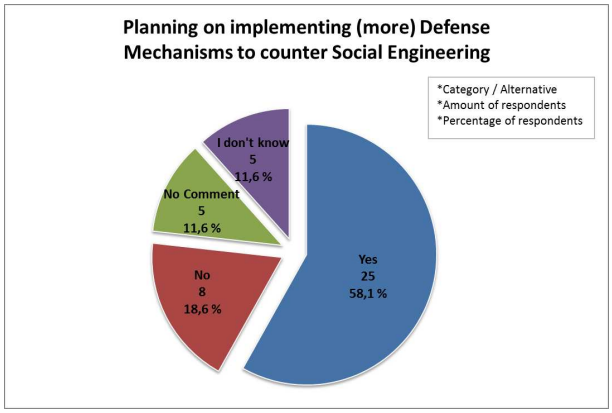

Figure 44: Planning to implement more Defense Mechanisms to counter Social Engineering

More than half of the organizations plan to implement more mechanisms to defend against Social Engineering. Here as well, 16 respondents mentioned in some way awareness as a defense mechanism they wanted to keep improving (not exactly the same respondents as in the prior question). Provided below are elaborations on what or why.

Short elaboration for those having answered *YES*

We asked: *Can you elaborate on what Defense Mechanisms you plan to implement to counter Social Engineering? (Detection/Prevention/Correction)*

Below is a summarizing of defense mechanisms the organizations plan to implement against Social Engineering. We also here divide them into *technically oriented* and *not technically oriented* defense mechanisms:

Technically oriented defense mechanisms

- DLP, Enhanced Surveillance on infrastructure units
- IDS
- SPF, DKIM, DMARC configuration on mail server
- Increased network and system monitoring
- Limitations in systems, event logging, security monitoring
- Better identity & access management platform & routines
- As new products and communication platforms are rolled out new defense mechanisms are incorporated
- More advanced firewall

Not technically oriented defense mechanisms

- Launch an awareness program for employees and measure the effect. Improve detection and reporting of attacks.

- Continue building a sound security culture. Maybe offer specific courses for likely targets of Social Engineering attacks identified through risk assessment
- Improving the quality of the awareness program
- Continued focus on awareness campaigns and introduce measurements of key metrics
- Mandatory training of all employees, were they need to sign that they have completed it
- Continue awareness programs
- Testing of Social Engineering

One respondent pointed out one of the challenges of defending against Social Engineering attacks (quoting):

> When it comes to Social Engineering it is difficult to find adequate controls due to the fact that Social Engineers misuse the established trust within an Organization/Society. Establishing to rigid controls will affect the efficiency of the Organization by more or likely distrusting all and everyone. Finding the right balance is very difficult in a business context where we're introduced to new tools used by the threats which we try to mitigate all known risks related to

We believe this is a very relevant and valid perspective of the challenges of defending against Social Engineering.

Short elaboration for those having answered *NO*

We asked: *Can you say anything about -why- you are not implementing (more) Defense Mechanisms to counter Social Engineering?*

Below is a summarizing of why not all organizations planned to implement (more) defenses against Social Engineering:

- "Built-in" defense mechanism (Scepticism)
- Management seems to be satisfied with the existing awareness program
- Probably have not realized how much it is present in the society
- There has been little focus on Social Engineering
- Mechanisms seems good enough at the moment, and further focus will be on awareness training
- Already have the most known/recognized security-solutions and monitoring in place

5.7.3 Do you think/know that you have countered an Social Engineering attack because of having Defense Mechanisms?

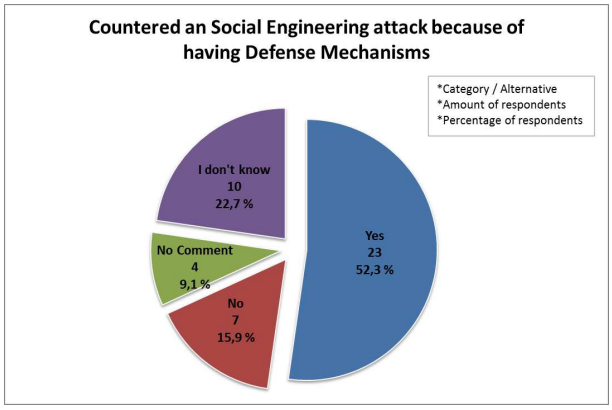

Figure 45: Countered an Social Engineering attack because of having Defense Mechanisms

Over half of the organizations meant their Defense mechanisms had prevented attacks from being successful. This question was however not causally connected to the question asking if mechanisms were in place (which it should have been in hindsight). Therefore, 22,7% (10 respondents, retrieved from the graph showing amount of organizations having implemented defense mechanisms) of those answering this question, did not have the nessecary prerequisit to answer it.

Therefore, if we assume that there were only 34 respondents that had the prerequisite to answer this question, and 23 of these answered yes, the correct amount of organization believing they have prevented attacks are 68%, not 52,3% (of those not having said they have no mechanisms in place). Though nevertheless of what is correct of those alternatives, it is nice too see that mechanisms implemented seem to work as intended. Below we provide some comments of those having answered yes.

Short elaboration for those having answered *YES*

We asked: *Can you elaborate on your Successful defense(s) of a Social Engineering attack?*

Below is a summary of successful defenses:

- Spam attacks are stopped in e-mail filter on a daily basis
- Employees says that concrete awareness makes them more sceptical to attacks
- Employees calls and inform that they have received e-mails
- End users receive Social Engineering attacks and forward them to IT-Security instead of clicking on them. This due to successful awareness campaigns.
- Sandboxing techniques of incoming emails has proven to be a very valuable defense. Some of the attacks have been of such "good quality" that even the most security aware employee would have been tricked

- During the last year, only one attempt has not been stopped and placed in quarantine. But, since the end users had received training, noone opened the malicious e-mail.

5.8 Conceived Security Risk of Social Engineering

We asked *How big of a security risk do you consider Social Engineering to be towards your Organization?*

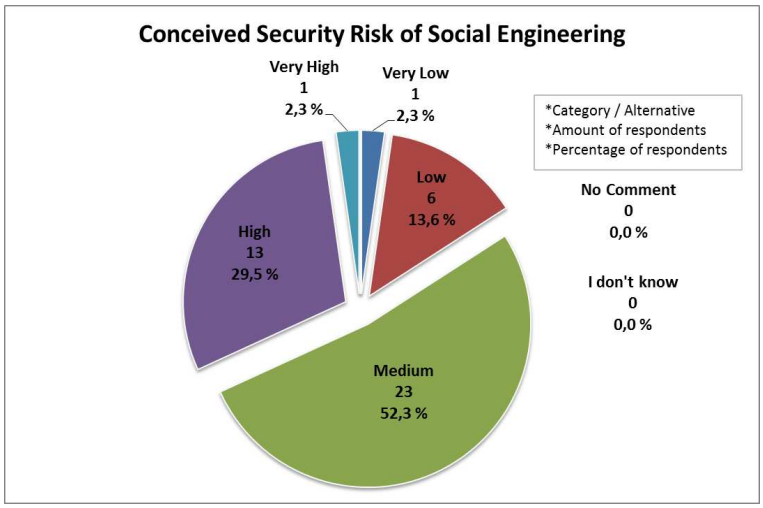

Figure 46: Social Engineering as a threat towards the Organization

The results show that over 50% of the respondent find the Security Risk of Social Engineering to be *medium*. In this scenario we must however keep in mind that the question basically consisted of 5 *real* alternatives, besides *No Comment* and *I don't know*. With the alternative *medium* being the median of those 5 alternatives, it could be perceived as being *the average* answer, neither high or low.

Though as the results show, twice as many respondents considered the Security Risk of Social Engineering to be *High* than *Low*. This essentially means that the respondent-pool is leaning towards Social Engineering being conceived as a medium to high risk. Furthermore however, this question is somewhat up to interpretations. Did the respondents consider the risk of Social Engineering *when it happens*, or the *overall* risk? (Likelihood multiplied with consequence)

Moreover, the Hawthorne-effect may be present. Having answered many questions about Social Engineering, economic consequences as well as defense mechanisms, one may begin to feel that Social Engineering is more risky than prior to having conducted the Questionnaire. It would have been interesting turning back time and asking this last question about the conceived risk, *at the beginning* of the Questionnaire, to see if it had been identical.

5.8.1 Criticism of Questionnaire (Self-evaluation of design)

We want to provide some hindsight-perspective of the Questionnaire, so that if others in the future choose to conduct a similar survey, they can build upon/improve our Questionnaire, instead of starting at scratch.

- Two respondents commented that no time period had been defined, resulting in them defining their own (lifetime and 2012). This does have a slightly negative impact on the validity of our results. Further, despite only two respondents commenting on this, there may be others doing the same thing, of which we do not know about. However, we *did* define a time period at the start of the Questionnaire, quoting: *For all questions; please consider events that has occurred* ***since the 1st of January 2011 and later.*** Though in light of all the information given to the respondents, this is easy to miss. We should therefore have added this information to every page of the Questionnaire.

- Though we are very pleased of all the input our respondents committed in the elaboration of their defense mechanisms, as mentioned in the prior chapter4.1, we would likely have been better of choosing a multiple-choice matrix with many mechanisms listed up, as well as an other-field for mechanisms not present. This would have made it more feasible drawing conclusion upon what mechanisms generally are used. In our Questionnaire as published, every respondent had to consider all possible defense mechanisms their Organization had, and further justify if they were relevant as answers. Then it is much easier saying yes/no to having a particular defense mechanism.

- As mentioned, the question *Do you think/know that you have countered an Social Engineering attack because of having Defense Mechanisms?* were not (but should have been) causally tied to the prior question asking whether or not one had implemented defense mechanisms.

- Though representing over 100 000 employees, the amount of respondents having answered is to low to generalize upon Norway. Though if only considering those organizations with 1000 employees or more, the pool would be more representable. We have in our final chapter9, mentioned that more respondents to the Questionnaire would have been beneficial, and might be the target for a similar survey in the future.

5.9 Summary of results

The results suggest that Social Engineering is a popular vector of attack in Norway, if not by all channels, at least by E-Mail, Social Networks and Websites. At the same time the results suggest that the consequences of a successful attack can be disastrous. Most organizations have implemented defense mechanisms against Social Engineering, but not every organization feel confident that they have successfully defended against a Social Engineering attack. Twice as many organizations say they conceive Social Engineering to be a High risk, as opposed to a Low risk, while roughly half of the organizations believe it to be a Medium risk.

On most of the graphs considering attacks, there were several respondents answering *I don't know*. This suggest that many organization do not have appropriate controls to detect and/or

report such events.

In the following chapter, we discuss how we can protect and defend ourselves from Social Engineering attacks.

6 Defending against Social Engineering

"If I gave this information to my worst enemy..."
- Kevin D. Mitnick

We started our Thesis by explaining what Social Engineering is, and how it can be used for malicious intentions. We deployed a Questionnaire targeting Norwegian Organizations, showing that Social Engineering attacks are definitely occurring, and even successful ones. Now we will discuss and present some of the defense mechanisms one can implement to defend one's organization against Social Engineering.

Illustrated by Bruce Schneier[10] with figure 47 below, is the *The Red Queen Effect Feedback Loop*. It consider how different species in the nature evolve to improved versions of themselves, in order to survive. In a security context we may refer to this concept as the *the-cat-and-mouse-game*. Social Engineering can also be considered as such. When one improve one's defenses, the adversaries improve their attacks. The challenge is that organizations need to defend against *all* attack-vectors, while the adversary only need to find one that is successful. Failing to defend against Social Engineering may pose losses to every aspect of the CIA-triangle[1].

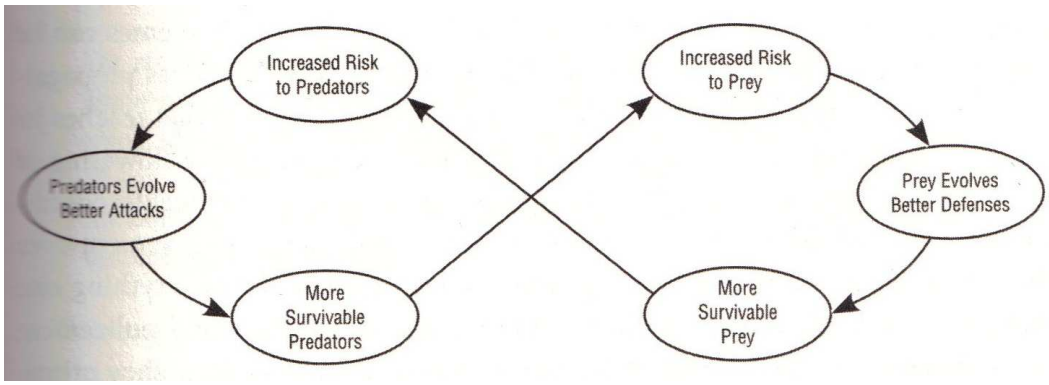

Figure 47: The Red Queen Effect Feedback Loop, Bruce Schneier

6.1 Defense Categories

In security we may divide defense mechanisms into three areas of focus; *Prevention,Detection and Correction*. Below we shortly discuss these areas from a Social Engineering perspective.

Prevention

In a Social Engineering context, preventive mechanisms should consider either technical measures, or procedures, that limit a Social Engineering attack from taking place/reaching a victim.

[1] CIA: Confidentiality, Integrity, Availability

In other words, the attempt of manipulation should not take place, or at least not be conceived by the victim.

Examples could be:

- Technical systems that verify the identity of a request before the request reaches a potential victim (like only allowing authenticated E-Mails being sent towards a system)
- Technical systems that blocks possible malicious code or/and URLs, (phishing-attemps) within all electronic communication (E-Mail, websurfing, SMS, etc)
- Strict Black & White procedures[2] that make no room for a possible victim *being understanding* when opposed by an adversary. Examples:
  - All employees must carry ID-badges - if not they should be confronted about it
  - All employees must use access-cards (or similar) when entering an organization's premises, the physical access control should only let one person enter for each verified identity. Some organizations take benefit of needing to verify one's identity both while entering a perimeter, as well as leaving. The access-control stops an employee from "logically" (as when identifying oneself with the access-card) leaving a perimeter when not having entered, or entering when not having left. (This to prevent borrowing or theft of such access-cards)
  - Using codewords to verify identified by phone. In no circumstance should information be released if the correct codeword is not given.

Detection

Mechanisms that are in place to *detect* possibly harmful activities (either malicious or natural). Intrusion detection systems are a good example - they only alert if they see packets that trigger certain signatures or anomalies, but are not necessarily doing anything to stop the packets from flowing to the victim. If put *inline*, usually the IDS can be configured to drop these packets as well (but is then operating as an *IPS*[3]) Another example is banks algorithm to detect unusual activity on our bank-accounts - if some possible fraudulent activity is alerted, the bank can continue to the prevention/correction phase; for instance calling the customer and verifying if the activity observed is legitimate.

Correction

At the moment a Social Engineer has manipulated an employee into divulging information, or performing some action, corrective measures should either block further malicious activity, or take action to limit the consequences of the activity having taken place. An example presenting the concept is from the 2nd of March, 2013, when the popular note-taking application Evernote was hacked[46]. The hackers got access to usernames, emails and enciphered passwords. In this scenario Evernote detected the attack, were not able to prevent it, but deployed an *corrective* action forcing every user to reset their password.

[2]Black & White procedures we define as strict procedures were it is beyond all doubt what to do, or not to do, in a certain scenario.

[3]Intrusion Prevention System

6.2 Multi-layered defense

Several entities suggest that one implement multi-layered defenses. Basically this means to not only have one single mechanisms defending against a certain attack, but several, so that if one were to fail, others mechanisms could still prevent a breach. We are not referring to redundant mechanisms, but rather different mechanisms implemented to counter different phases of an attack. A theoretical example:

1. Not having phone numbers only meant for customer publicly online on the organization's website
2. Call-in-procedure: asking for codewords when a customer calls in to the organization
3. Logging for what information was released when, and preferably by who
4. WEB-filtering mechanisms, IDS/IPS, etc.
5. Stand-by Incident Response Team (IRT)

The concept is that by limiting the amount of people knowing a phone number meant for customers, one also reduce the amount of *non-customers* calling in. Of course, *security by obscurity* is not something that is considered *effective* security, but nevertheless makes it harder for an adversary gathering needed information.

If an adversary is able to find the number, he still needs to know a codeword. If able to get information/commit requests without this codeword, there are logging-mechanisms in place to detect suspicious/anomalous behaviour. If an employee, despite not having received a codeword, comply to the adversary's request and for instance navigate to a malicious website, the WEB-filtering or other blocking-mechanisms would stop malicious code from being run in the context of the employees computer. If the attack were to be successful, but detected, the event is flagged as an incident and given to the IRT which respond as they find appropriate.

Each such layer of defense mechanism lessen the likelihood for a successful breach and/or the consequences if a breach were to happen.

6.3 Literature and earlier research

Most studies and literature that investigate aspects of Social Engineering, also make some effort into describing possible defense-mechanisms. The nature of Social Engineering, being it attacks the human mind, makes it challenging defending against. If a website is vulnerable to SQL-injection attacks, attempts to secure it can be to sanitize input-fields. It is of course not *that* easy - every day new vulnerabilities are discovered. But generally IT-Security experts can perform penetration tests towards an organization, for thereafter reporting to IT-personnel regarding what needs to be done to be more secure, for instance by updating and patching all servers and clients. (Also not that easy in today's environment, were an update may leave applications incompatible with each other, resulting in downtime.)

How can we prevent successful attacks towards the human brain? Though being quite harsh, some state that *There is no patch for Human Stupidity*. There is some truth to that, not that one

cannot patch stupidity, but the fact that defending the human brain is intangible compared to defending a specific application. So what measures can we take when there exist no tangible input-field to sanitize?

The majority of literature and earlier studies point towards *Security Awareness* as a crucial factor when to defend against Social Engineering.

One study, conducted in 2010 by L.J. Janczewski and Fu Lingyan, and published at IEEE, is *Social engineering-based attacks: Model and new zealand perspective*[47].

Their study investigated what vulnerabilities Social Engineering exploit, what techniques exist, consequences, as well as defenses against Social Engineering. Though having some resembles to our research questions, they mainly considered New Zealand as their scope. They (also) conclude with user-awareness as a critical factor in the defense against Social Engineering, quoting:

> Both the literature review and data analysis have suggested that people are the weakest link in security control systems. In addition, lack of security awareness and psychological weaknesses of people are the main reasons that social engineering-based attacks succeed.

They interviewed 25 individuals within various areas of IT:

> 12% of the participants pointed out that most security technologies are incapable of detecting and preventing social engineering as social engineering bypasses technical controls via manipulating people who are managing them.

Further they say that Social Engineers take benefit of victims being *unsure*, whether or not a particular action is correct to do. Example being unsure of whether or not to let a person enter the building when when not having sufficiently identified themselves. This would suggest that strict procedures in such circumstances are needed (Black & White: if no identify can be verified 100%; do not let in.)

They also suggest the following recommendations to defend against Social Engineering:

- Access control to limit physical access to building
- Multi-factor authentication may prevent unauthorised access
- Implementing a Security Policy that sets the line of how people should behave in the organization, consequently removing the *uncertainty* of which a Social Engineering preys upon.

44% of the interviewed claimed that people in New Zealand generally have a higher level of social trust, which implies they are more vulnerable to Social Engineering-based attacks. 32% of the participants mentioned that Social Engineering was overlooked in a security context. (Our Questionnaire suggest the similar; 22,7% not having defense mechanisms, more or less by Social Engineering not having been recognized as a big enough threat). (5.7.1)

Another paper, specifically looking into *Phishing* as a Social Engineering technique, written by Jingguo Wang and titled *Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email*[11] also concluded with Security Awareness being important:

- Knowledge of email-based scams increases attention to phishing deception indicators, and directly decreases response likelihood

- The implication of the study is that attention to visceral triggers, attention to phishing deception indicators, and phishing knowledge - play critical roles in phishing detection."

Were Wang looked into what decided for a phishing attempt being successful, Snekkenes et al. points out three variables that the outcome of a Social Engineering attack is depended upon, in their article *Measuring Resistance to Social Engineering*[36]:

- the adversary's (both white and black hats) ability to carry out the attack.
- the victim's ability to detect the attack.
- other factors outside the control of both adversary and victim.

Reducing the adversary's ability is not a feasible task, as one generally do not know who the adversaries actually are. However, implementing strict procedures, technical measures, as well as not being to public with certain information may limit the adversary's ability to deploy an effective attack in the first place. The bulletin about the victim's ability to detect Social Engineering consider mainly security awareness, but also other technical measures that may for instance flag an E-Mail as potentially malicious.

In NorCERT's first Quarterly report of 2012[48], they discussed Social Engineering being used more and more as targeted attacks towards specific employees in organizations. Below is a list of their recommendations for defending against Social Engineering (translated to English). All these advices consider security awareness.

- Admit that the organization is handling sensitive information that may be of interest to others.
- Understand that everyone can be a target of Social Engineering or targeted attacks.
- Admit that *you* have information that can help an adversary towards his final goal.
- If something is to good to be true it usually is.
- Be sceptical towards E-Mail
- Be sceptical towards attachments and links you receive
- Ask yourself why you are receiving E-Mail from the sender
- Did you expect an E-Mail like this?
- Is there a logical reason for you receiving this E-Mail?
- Have your organization cooperated with the sender before?
- Which other recipients is the E-Mail sent to?
- Have anyone you know also received this particular E-Mail?
- Do you have the opportunity to verify that the E-Mail is benign (for instance by calling) - then do it!

6.3.1 Interview with Øivind Høiem, CISA, CRISC

We were given the privilege of interviewing Øivind Høiem about Social Engineering. Øivind Høiem has 10 years experience within Information Security, working at Statoil. He has worked extensively with the development of Security Awareness programs and are currently (as of 2013,May) working at Uninett in Norway as a Senior Advisor within Information Security.

Høiem has, amongst other, the following recommendations and comments regarding how to defend against Social Engineering, and about Security Awareness in general:

- Awareness is one of the most important weapons against Social Engineering
- Ask employees: "What is the next security incident that will give our organization negative PR" (stimulate users to think out-of-the-box)
- Users need to understand *why* one have to do something a certain way (what are the consequences if not?)
- Users need to *understand* security, they need to understand what can happen, and how it may affect them
- Security requirements must be realistic, they need to function in practice and not just be theoretical.
- Security-personnel must change the way they communicate: *Don't say no, say how*
- Perimeter defense: If a stranger is observed within the perimeter of the organization the culture must be to confront this person

Roar Thon, senior advisor at Norwegian National Security Authority (as of April, 2013) mention in a blog from his attendance on the RSH conference[49] in 2013, that both Belani og Murray agreed that the fundamental problem with security awareness programs is that security-personnel is trying to teach end-users about security. The angle of attack therefore becomes inefficient. They both argued that it would be best to not focus on details in the Security Awareness program - it should be comprehensible by all users.

The data gathered from our Questionnaire suggest that most the Organizations have several defenses implemented. We see that it seem to be *natural* distinguishing between *technical* and *non-technical* measures. We have already discussed Security Awareness being an important factor for defending against Social Engineering (which also some of our respondents explicitly say is the root-cause for having defended against a Social Engineering attack). Some respondents also points out sandboxing of incoming E-Mails as an effective defense mechanism. Please refer back to the analysis-chapter for more thorough listing of the mechanisms of our respondents.5.7

6.3.2 SELM - Social Engineering Land Mines

In late 2012, David Gragg wrote a paper titled *A Multi-Level Defense against Social Engineering*[32], published by SANS, in which he proposed the term *SELM - Social Engineering land mines*. If Social Engineering was not already a fancy term, adding *land mines* behind it makes it even more. The term is head on however. A land mine explode when some entity move over it. SELM also consider this, not physically blowing someone up of course, but making an organization aware of something currently happening. *Honeynets* and *honeypots* are more or less synonyms to it. They are deployed to intrigue an adversary into attacking them, instead of other systems, while at the same time raising the red flag of something "phishy" going on.

Gragg propose some ideas: (this concept is only limited by one's own creativity)

- Having a person who's job-description concerns knowing everyone on the floor - if a stranger would enter the floor, the person should confront him/her
- Bogus Question - asking a seemingly legit question that one know there exist no valid answer for, like "How is your dog?". A Social Engineering would very likely say that the dog is fine, or it currently being ill (to appear more valid). The person asking the question do however already know that the supposed person calling in do not have a dog, which implies that a Social Engineer is at hand.

6.4 Social Engineering Audits

As mentioned by Snekkenes et al. in *Measuring Resistance to Social Engineering*[36], performing Social Engineering tests are an effective way of measuring employees current level of user awareness. Further, such tests help users understand the potential consequences of Social Engineering, which further help justify investing resources in defense mechanisms.

There exist several entities in Norway delivering Audits within Social Engineering, for instance; Secode, Mnemonic, PWC, Ernst & Young and Watchcom.

When conducting such audits it is important making sure that personnel, which have been targeted/attacked, is treated anonymously. Audits should aim for finding relevant vulnerabilities into an organization as well as increasing awareness of security, not prove that employees are prone to manipulation, or *point fingers*.

Ketil Granbakken, Salesdirector at Secode (as of May-2013), say they perform roughly 12 Social Engineering Audits each year. Often the same customers periodically order audits to verify that mechanisms implemented to defend against Social Engineering are effective. He further says an average Audit cost between 120.000 and 250.000 Norwegian Kroner.

6.5 Summary of defenses

Our review of literature and earlier research suggest that security awareness is a crucial factor for defending again Social Engineering. It is comforting to see that many of our respondents are working constantly with awareness, or have it on the agenda for the upcoming future. But how should one actually proceed when developing a Security Awareness program? Next chapter we have dedicated for discussing Security Awareness.

7 About Security Awareness Programs

To cope with Social Engineering attacks, literature, studies, professionals, and our Questionnaire, suggest that one need to develop a Security Awareness program that makes users more aware of potential threats. In this chapter we will elaborate on Security Awareness.

7.1 It used to be expensive making things public

It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public. - Clay Shirky, professor at N.Y.U.

Shirky sum it all up in those two sentences. Before it was intriguing being able to share information, pictures, and everything that happened in our lives. Now, with for instance Facebook and Twitter, we are urged to keep a lid on all things we priorly shared - because when it is uploaded onto the Internet, there really is no way back. People share with their fellow "friends" on facebook that they are going away for holiday - while reading in between the lines, they are actually saying one is welcome to rob their homes.

One may answer relentlessly to an email which appear to be coming from the same email-domain as oneself, while it in practise, really are someone deliberately using a look-alike-rogue-address to gather sensitive information. We like to help each other, and therefore we hold up the door for the poor guy stressing to hold up the cardboard-boxes.

The list go on and on, and with good reasons. Most of the time it is not a guy that wants to steal sensitive information, but just someone that tries to do their job. We cannot suspect everyone of being after harms way, then we would be too occupied to actually do our job.

7.1.1 Like putting up a steel wall

There is today a strong focus on technical defences, like firewalls and for instance two-factor authentication that is meant to prevent unauthorised access. But what these tools often do, is to keep everyone not holding the correct credentials out in the freezing cold - but when one do have correct credentials - one is instantly invited into the hot zone.

It is like putting up a huge steel-wall with a vast amount of guards defending it and scouting for intruders. There is however no walls at all behind this wall, so when someone is able to enter, they can do whatever they want. This is of course not always true; having installed internal Intrusion Detection and Prevention Systems helps counter malicious activity. The same concept is however applied to the physical world; when a person is already inside a security-perimeter, he is considered to be "benign" by other employees. This is especially true for larger organizations were it is not feasible for every employer to know one another.

Security Awareness reflects how an individual handles potential security-risks in his/her environ-

ment. For instance knowing that emails claiming that one have won billions of dollars, actually are attempts to steal ones credit-card number. However, not all scenarios are that transparent. We need to educate ourselves, and our employees, to also recognise more sophisticated threats. In order to do this we need a method of approach, we need a Security Awareness learning-program.

7.2 Documented Successful Methods

Most literature in the field of Security Awareness points out that there are no single way of conducting such a program, that will fit all environments and employees. This is what makes it a rather tough nut to crack in contradiction to for instance more technically oriented fields, like firewalls, or developing new cryptographic software. This doesn't mean that this work is easy, it just means that there is a lack of scientifically proven methods on how to make users aware of possible security pitfalls. If asking a specific organization about effective methods, they will surely have some examples, but chances are that these would not be suitable for another organization.

There exist different ways of developing a Security Awareness programs. Some may think that some kind of lecture for all employees at once is the best thing to do. Someone else may use short and concise messages on paper-strips, for instance on the mirror in the bathroom, or by the coffee-machine. Some may make an interactive electronic program that all employees need to go through, for thereafter answering a couple of questions.

7.2.1 ENISA - Survey: Current practice and measurement

In 2007, the European Network and Information Security Agency (ENISA), made public a report; *Information security awareness initiatives: Current practice and the measurement of success*[50]. This report highlights the general trend of how a Security Awareness program is conducted in practise, as well as what communication channels have showed to be the most effective implementing. The report has considered the experience of 67 organizations and governments within the European Union (EU), with staffing ranging from 50 to 10 000 employees. Despite the report being several years old, methods has likely not changed much. However, it is important to keep in mind that social media like facebook and twitter is growing rapidly, and should perhaps also be mentioned.

On the next three pages one find some of the results retrieved from the mentioned report by ENISA.

Below, in figure 48, one can see the popular methods of arguing for the costs of conducting Security Awareness programs. One see that *Compliance requirement* is used by the majority of the respondents. This corresponds well with David Lacey's saying that one should use mandatory compliance requirements for what it is worth, in order to justify costs for Security Awareness programs (from his book *Managing the Human Factor in Information Security*[45]).

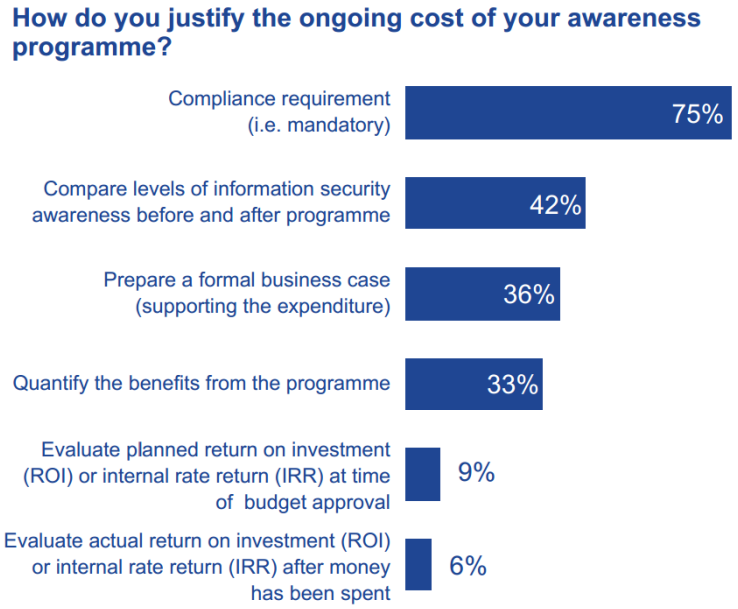

Figure 48: Means of justifying costs for Security Awareness programs, ENISA

Following, in figure 49, is an overview of what is generally done when conducting such a program. Policies and similar is mostly used, together with guidance on intranet sites. There seem to be some introductory security awareness training when new employees arrives, but the more *continuous, ongoing* training is less used.

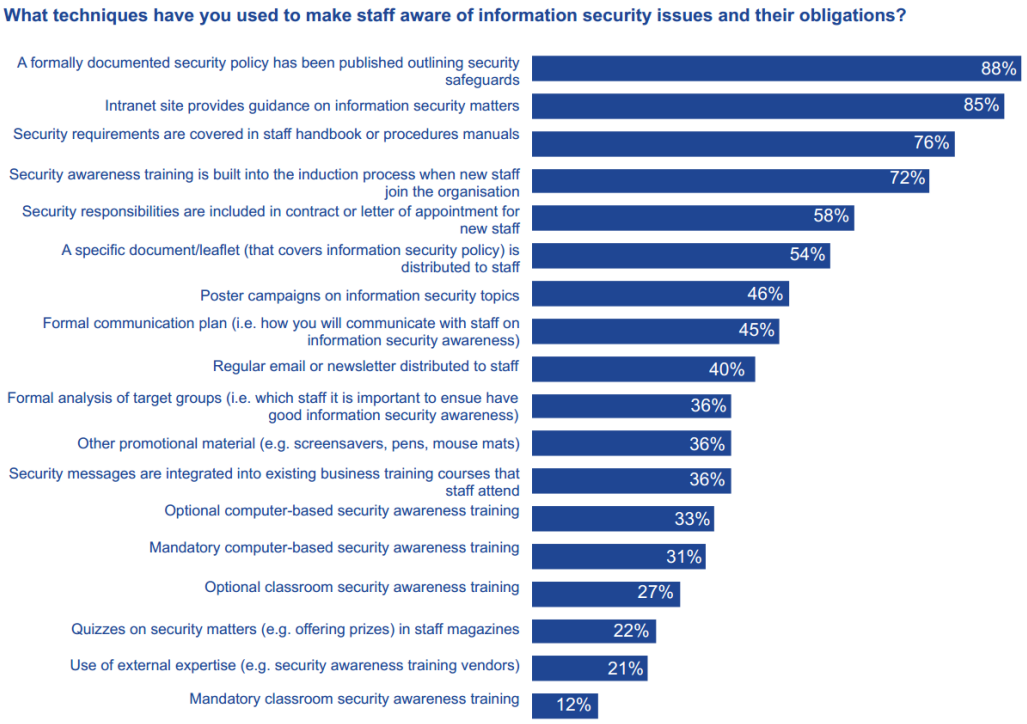

Figure 49: Techniques used in Security Awareness programs, ENISA

Following, in figure 50, an overview of what techniques has proven to improve Security Awareness *effectively* within an organization. What is interesting, is that classroom-training is concidered being one of the most effective training methods, but the figure 49 above shows that it is the least used. This is likely because of the costs of conducting it. One must keep in mind that all time the employees use at such programs, are *lost man-hours*. It therefore needs to be justifiably. What is also interesting, is that despite, as mentioned above, that policies and etc. is often used to teach awareness, there is a disagreement in the efficiency of it, as shown in figure 50

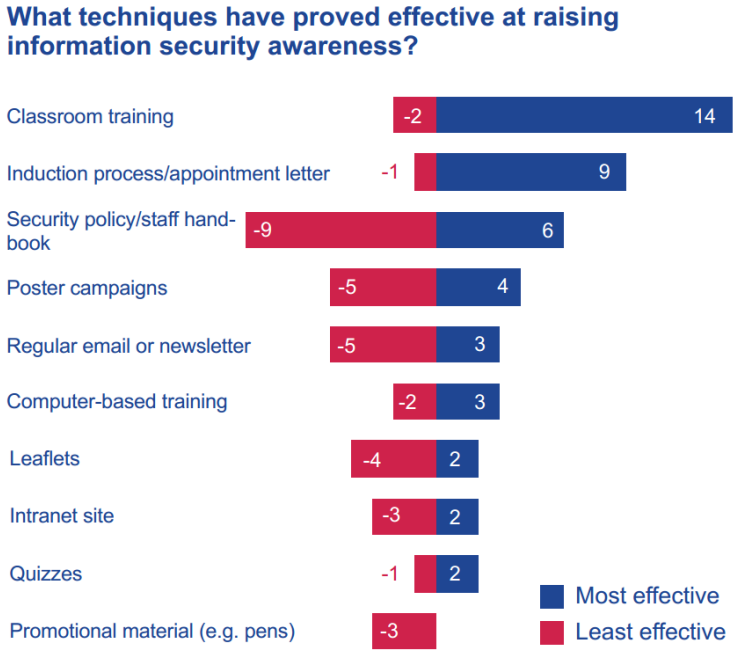

Figure 50: Techniques proved to improve Security Awareness, ENISA

7.2.2 Alternative method for improving Security Awareness

Bjørnar Prestaasen, a graduate student at Gjøvik University College in 2011, researched in his Master Thesis; *Improving Security Awareness and Ownership using a method based on Action Research*[51], an alternative method for improving Security Awareness. He investigated if participating in an intervention regarding Security Awareness would improve the Awareness of its participants. The employees were then able to (meant to) participate, ask questions, and share thoughts. The experience was considered to be positive and successful for the participants. Using interventions for improving Security Awareness within an organization may therefore be a viable approach.

7.3 Critical Success Factors

7.3.1 Knowledge, Attitude & Behaviour

As Security Awareness regards the human mind - and we all have a different one, it doesn't come as a surprise that there exist few specific, successful and perfect ways of developing, and performing a Security Awareness program. It is all about the context. As Lacey puts it:

> Before we can design any effective campaign, we have to find out what the people in our target audience actually know and think about the subject, as well as how they're likely to behave, especially when you're not watching them.

Take a good note of the (crucial) last part; *especially when you're not watching them*. It is not that employees cannot be trusted, but people behave differently in different environments. When one's boss is hanging over one's shoulder one sure strive to not do a mistake, but may be more relaxed when being alone. One need to make sure that employees behave as one want, *especially* when one are not watching them. In other words; one need to tailor the Awareness-program to the recipients so that the likelihood for this increases. Lacey also pinpoints three important *categories* of Security Awareness:

- Knowledge
- Attitude
- Behaviour

One may likely be able to use other terms, and even divide them more up, but the concept will still remain; It doesn't matter if ones employees are highly knowledgeable about how to handle sensitive information, if they don't rely on, and use this knowledge in practise.

People may for instance know that smoking is bad, but they still smoke. They may even want to quit smoking -but they don't. When it all comes down to nothing they are, in fact, still smoking. They have changed their knowledge, they have changed their attitude, but they have not changed their behaviour. One should therefore aim towards changing the behaviour of employees, and not just the knowledge and/or attitude.

7.3.2 Implementing an Effective Strategy

As mentioned in the paper; *Security Awareness - Implementing an Effective Strategy*, written by Chelsa Russel and published by SANS[52], it is impossible to eliminate risk. The main objective of Risk Management is to mitigate the risk, to reduce the risk to an acceptable level for the organization. Despite written 10 years ago (2002), the same account today, also for Security Awareness challenges (which arguable is also to be considered covered by a Risk Management process). One cannot make it impossible for an unknown adversary entering a building, or one could try, but the business would certainly be disrupted in terms of inefficiency, needing to perform thorough checks/screening of everyone entering. But even then, what if someone stole the identity of one of the employees, stole their business-identity-card, and even performed plastic-surgery to look like the person? A quite absurd idea, true, but would nevertheless very likely surface be a successful attack. It is important acknowledging that one cannot achieve being 100% secure.

The primary objective with a Security Awareness program, as mentioned by Russel, is to:

> Educate users on their responsibility to help protect the confidentiality,availability and integrity of their organization's information and information assets. Information security is everyone's responsibility, not just the IT security department.

Russel also mentions that Security Awareness can be broken down into *awareness* and *training*. The Former corresponds to educating the users in best-practises (Knowledge & Attitude), while the latter to go more in-depth in how to behave (Behaviour).

She also mention recommendations for developing a Security Awareness program:

- Establish Security Policy
- Identify Current Training Needs
- Obtain Support
- Determine Audiences
- Define Key Messages
- Define Available Communication Vehicles
- Develop a Strategy for Implementation
- Awareness Strategy
- Training Strategy
- Ability to measure

To continue, Russel also mention some obstacles that needs to be overcome for a successful Security Awareness program:

- Teaching an old dog new tricks
- Security is an information technology problem, not mine
- Implementation of new technology
- One-size-fits-all
- Too much information
- Lack of organization
- Failure to follow-up
- Getting the messages where it counts

- Lack of management support
- Lack of resources
- No explanation of *why*
- Social Engineering

7.4 Example of a Security Awareness program

In 2007, SANS released a paper, "Making Security Awareness Efforts Work for You", written by Rebecca Thurmond Fowler[53]. This paper describes a Security Awareness program developed and implemented by *The Division of Information Technology at the University of Missouri-Columbia*. The program had two main parts; *formal awareness training* and *activities centered around monthly security topics*. They had three goals:

- To change the way people think and act when it comes to information security
- To continually address the importance of security in the campus environment
- To keep users informed of the rapidly changing security landscape

In other words, more or less what every organization should aim for.

What is quite interesting about this group, is that they decided to view security as a *product*, something they needed to *sell* to their users. The product therefore had to be so interesting and easy to grasp, that users would be interested in, and feel inclined towards spending what was needed in order to get this product. The currency would be their time and energy committed to be aware of security threats.

In order to gain this sort of break-through, they initially started by developing a logo, a symbol of security, that when was seen, always would have sensible advices regarding Security Awareness. Below, in figure 51, is the logo named "Key Guy" used in the program (made by, and the property of the University of Missouri-Columbia)

Figure 51: Key Guy

The logo were used together with tailored messages in several different arenas, like newsletters, newspapers, posters and displays. Their aim was to make people associate the logo with

something that was important for *them* - the end-users. Take a moment to analyse the logo, and one will see that quite some thoughts has been put into the development of it.

Lacey also wanted people to grasp this concept. He wanted developers of Security Awareness programs to see that one need to apply marketing-methods to really kick of such a Security Awareness campaign. Imagine watching TV when a new commercial runs. The commercial have no sound, and only show a newly invented black metal box for a few seconds, and then ends. What is it? Why should one buy this product? Is it even for sale? This commercial would surely not make people jump off their couch and visit the nearest electronic store. Maybe they would grab their Ipad and see if they could find out what it really was, just to satisfy their curiosity - but one would not think about buying it, for the simple reason that one do not know what it is.

The same accounts for Information Security. One have to make users understand that they *need it* - and, one may have to create this need.

In the paper, Russel also describes several potential vehicles for transferring the *messages*:

- Broadcast e-mail
- Targeted e-mail
- Broadcast voicemail
- Company newsletter
- Departmental newsletter
- Intranet
- Printed materials - posters, bulletin boards and brochures
- Face-to-face - meetings, presentations, training and Security Conference/fair
- Library - videos, books and interactive presentations
- Reminders - login-banners, marketing paraphernalia (mugs, pens, mousepads, keychains, sticky-notes, etc.)

What is interesting with these vehicles is that they corresponds quite well with those used in general marketing.

Lew McCreary, Content Expert Faculty of the CSO Executive Council, also states, in an article on csoonline.com; *Security Awareness Programs: Now Hear This!*[54], that marketing is important for Security Awareness, specifically marketing *about the importance of security as both the guardian and enabler of core business value*. In this article it is also stated that a challenge is how to communicate with the various kind of recipients, as *you have different levels of expertise you have to talk to*.

7.5 Online Gaming

People like games. They enjoy playing them, and what they enjoy more than playing them, is winning. On onguardonline.gov[55], several games, (among others) that aim to increase ones Security Awareness, are available for download. Such a game should be considered a very cost-effective approach for improving Security Awareness - one make it once, put it up on the In-

tranet, and then everyone can play it. However, it is important to understand how to reach the addressee, or else the attempt might be a failed one.

On the next page one can see some cut-outs from some of the games (and videos) available at (and the property of) OnGuardOnline. It is not hard to understand that when Security Awareness messages are conveyed in this way, it is much more fun and interesting spending time on.

Figure 52: Game: The Case of The Cyber Criminal

Figure 53: Game: Mission: Laptop Security

Figure 54: Game: Invasion of the Wireless Hackers

Figure 55: Game: Invasion of the Wireless Hackers - in game

Figure 56: A Video about phishing: Guy caught after trying to "Phish" after information - notice the fin

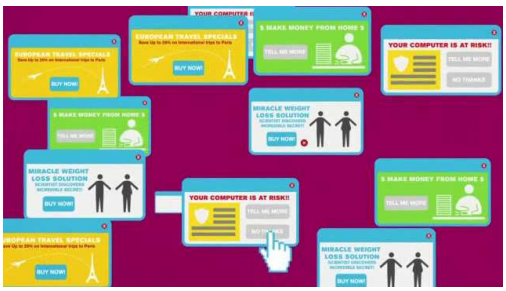

Figure 57: Video: Protect Your Computer From Malware

Similar to the video/games on the prior page, SANS has also within the *Securing the Human*-project developed *Security Awareness Modules*[56] that can be used to increase awareness:

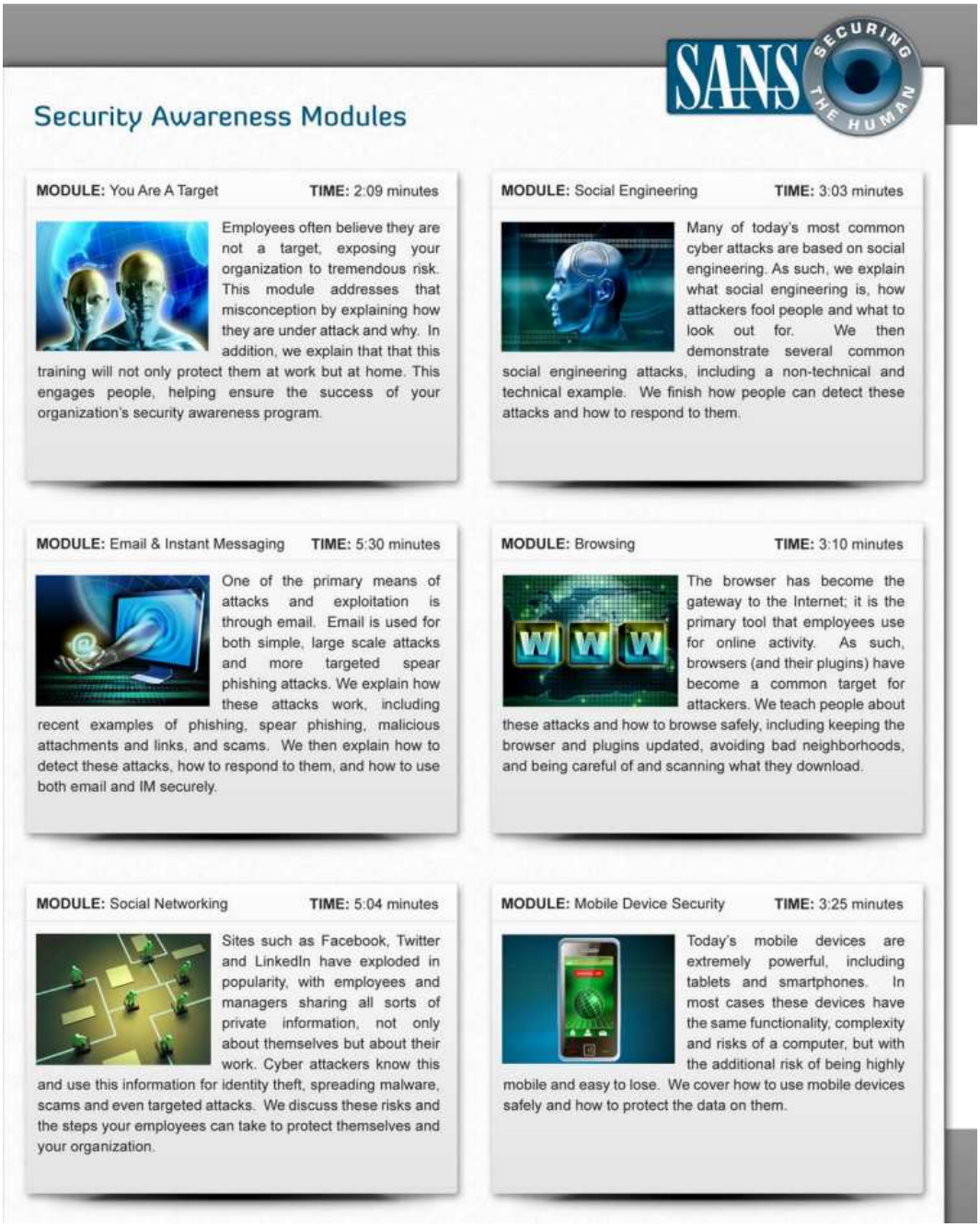

Figure 58: Example of Security Awareness modules in the Securing the Human project

8 Summary

In this Thesis we have looked into some of the principles as to why we are as prone to Social Engineering attacks as we are, like Cialdini's *Six Human Tendencies*[4].

We initially wanted to find out if Social Engineering is indeed a vector of attack that is used to target Norwegian Organizations. Most literature and earlier research suggest that Social Engineering is a current, realistic threat. This is further backup up by our Questionnaire which shows that not only are attacks deployed through all channels we defined, successful attacks can result in losses of several millions of Norwegian Kroner. Although most organizations do not consider Social Engineering to be a High threat, the results still suggest that most have taken precautions to limit the likelihood of a successful attack, for instance by having focus on Awareness training, as well as implementing technical measures in all three categories of defenses.[1]

Further it seems as those vector of attacks that do not require oral communication with a victim; (i) E-Mail, (ii) Social Networks and (iii) Websites are the most heavily used by adversaries. This is likely because of having high ROI[2] for the adversaries in question. They can commit as much time as they want before sending it out, as well as being able to reach a vast amount of people. Another perspective is that one are not dependent upon oral communication skills when relying on written communication. The potential *price* if making an effort to penetrate an organization physically may be larger than the general E-Mail being sent, but the risk taken is several order of magnitude larger as well.

As most professionals within Information Security have already conveyed, Security Awareness is a must when to defend against Social Engineering. There need to be constant focus on the emerging threats and a culture within the organization to report suspicious behaviour and activity. Still it is important to also take benefit of the more tangible technical defense mechanisms one can implement, for instance Mail-washers and IDS/IPS-solutions. Lastly, Black & White procedures should be implemented and anchored in top-management of the organization, removing responsibilities away from end-users. Users need to feel confident when saying *no* to a potential adversary, referring to the agreed upon procedure.

[1] Preventive, Detective, Corrective
[2] ROI: Return On Investment

9 Future Work

9.1 More respondents to Questionnaire

On of the limitations of our Questionnaire were that it was only answered by 44 respondents/organizations. This is to small a number being able to generalise for entire Norway. Though as we stated in our analysis, as the organizations consist of as many employees as they do, the Questionnaire essentially represent over 100 000 employees. Still it would have been interesting reaching more respondents than we did.

9.2 Framework for developing awareness programs

Many authors points out tips & tricks for defending against Social Engineering. It is however not always easy converting these advices into something that the organization can use. We thought about finding an easier approach for organizations to defend themselves. Initially our ambition were to develop a Security Awareness program that focused on Social Engineering. This way an organization could instantly benefit from our work, not needing to develop such a program themselves.

However, as discussed in our chapter about Security Awareness programs (7), it is not always straight forward adopting an Awareness program that is not tailored towards the organization in question. Few organizations are alike, and most have different assets to defend, as well as different risk-cultures and working-cultures. Because of this, we instead of making an awareness program, looked into the possibility of developing a *framework* for developing an awareness program.

Our aim with this framework were that it should be considered a *go-to* document when developing an awareness program. It should provide enough information and tips for an organization not needing to attend different sources. If the information present in the framework were to be limited, it should point towards were one could find more comprehensive information.

We further considered making the framework based on *modules*, where Social Engineering was one, and for instance the handling of sensitive information another. One would then be able to extend the framework as one progressed with more best-practises.

Looking at the ISO27001[1] & ISO27002[2] standards for guidance, we thought about applying the same principles to the framework. A comprehensive list of best-practises within security awareness programs and how to implement them. To use the framework, one would traverse through it,

[1] ISO27001: Information technology — Security techniques — Information security management systems — Requirements

[2] ISO27002: Information technology — Security techniques — Code of practice for information security management

roughly in the same manner as one progress through ISO27002. For each bulletin/best-practise one mark it as applicable or not for one's organization.

When having gone through the entire list of possible "controls", one would be confident that one have considered the most valid and recognised best-practises within security awareness, gathered together on the experience of others.

This was as far as we came into exploring this thought. We have not thoroughly looked into pro's and con's of such a framework, and others may even already have developed something similar.

We believe it would be interesting going down this road, investigating whether or not such a framework is something that could benefit organizations.

9.3 Critical points in attacks

One approach to figure out how to defend against Social Engineering could be to find critical points in various attacks, that is, a certain point at which one is most likely to be able to distinguish a legitimate request from a malicious attack.

An example is if someone asks for one's password, for any reason. Red flags should immediately be raised. Similarly one can have defined certain types of information within an organization that never would be asked for over certain channels. If someone did, they were to be considered malicious.

Bibliography

[1] Wikipedia. Kevin mitnick. http://en.wikipedia.org/wiki/Kevin_Mitnick. Last Accessed: 2013-06-01.

[2] Mitnicksecurity. Mitnick security consulting, llc. Mitnicksecurity.com. Last Accessed: 2013-06-01.

[3] The University of New South Waled, Sydney, A. Unsw australia, school of psychology. http://www.psy.unsw.edu.au/. Last Accessed: 2013-06-01.

[4] Cialdini, R. B. 2007. *Paavirkning - Teori og Praksis*. Abstrakt forlag.

[5] NorSIS. Phishing via facebook. http://www.norsis.no/nyheter/2010-03-03_Phishing_via_Facebook.html. Last Accessed 2013-04-25.

[6] Trusteer. Measuring the effectiveness of in-the-wild phishing attacks. http://www.opensourceintelligence.eu/ric/doc/Phishing-Statistics-Dec-2009-FIN.pdf. Last Accessed: 2013-06-01.

[7] Norge, F. 850 000 norwegians never visits their bank. http://www.fno.no/Hoved/Aktuelt/Sporreundersokelser/Dagligbankundersokelsen/dagligbankundersokelsen-2013/850-000-nordmenn-gar-aldri-i-banken/. Last Accessed 2013-04-25.

[8] Checkpoint. The risk of social engineering on information security: A survey of it professionals. http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf. Last Accessed 2013-05-19.

[9] social. Multi-tiered social engineering attack. http://www.social-engineer.org/interesting-se-articles/high-profile-xbox-live-accounts-hacked/. Last Accessed: 2013-04-14.

[10] Schneider, B. 2012. *Liars & Outliers Enabling the thrust that society needs to thrive*. John Wiley & Sons, Inc.

[11] Wang, K. 2012. Phishing susceptibility: An investigation into the processing of a targeted spear phishing email.

[12] McClure, J., Ames, W. I., Jr., T. F. M., & Gouin, J.-L. 2002. A system and method for enhanced psychophysiological detection of deception.

[13] Wikipedia. Microexpression. http://en.wikipedia.org/wiki/Microexpression. Last Accessed: 2013-05-24.

[14] Hadnagy, C. 2010. *Social Engineering - The Art of Human Hacking*. John Wiley and Sons Ltd.

[15] Li, W., Zinbarg, R. E., Boehm, S. G., & Paller, K. A. 2008. Neural and behavioral evidence for affective priming of unconsciously perceived emotional facial expressions and the influence of trait anxiety.

[16] Security, H. Deception detection - identifying hostile intent. http://www.dhs.gov/deception-detection. Last Accessed: 2013-05-09.

[17] Security, H. Experimental testing of project hostile intent technology. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_phi.pdf. Last Accessed: 2013-05-09.

[18] Evans, N. J. 2009. Information technology social engineering: an academic definition and study of social engineering - analyzing the human firewall.

[19] Bandler, R. Home page of richard bandler. http://www.richardbandler.com/. Last Accessed: 2013-05-13.

[20] Wikipedia. Richard bandler. http://en.wikipedia.org/wiki/Richard_Bandler. Last Accessed: 2013-05-13.

[21] Grinder, J. The home page of nlp co-creator john grinder and carmen bostic st clair. http://www.johngrinder.com/. Last Accessed: 2013-05-13.

[22] Wikipedia. John grinder. http://en.wikipedia.org/wiki/John_Grinder. Last Accessed: 2013-05-13.

[23] Bliemeister, J. 1988. Empirical verification of central theoretical constructs of neurolinguistic programming.

[24] Bradley, E. & Heinz-Joachim, B. 1985. Bandler and grinder's neurolinguistic programming: Its historical context and contribution.

[25] Sharpley, C. F. 1984. Predicate matching in nlp: A review of research on the preferred representation system.

[26] Sharpley, C. F. 1987. Research findings on neurolinguistic programming: Nonsupportive data or an untestable theory?

[27] Druckman, D. & Swets, J. 1988. Enhancing human performance: Issues,theories, and techniques.

[28] Bergen, C. W. V., Soper, B., Rosenthal, G. T., & Wilkinson, L. V. 1997. *Selected Alternative Training Techniques in HRD*.

[29] Andreas, S. Steve andreas - nlp blog. http://realpeoplepress.com/blog/. Last Accessed: 2013-05-24.

[30] Mitnick, K. D. & Simon, W. L. 2003. *The Art of Deception - Controlling the Human Element of Security*. John Wiley & Sons Inc.

[31] Lisman, J. & Sternberg, E. J. 2013. The pilot and autopilot within our mind-brain connection.

[32] SANS. A multi-level defense against social engineering. http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920. Last Accessed 2013-04-29.

[33] wired.com. How apple and amazon security flaws led to my epic hacking. http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/. Last Accessed: 2013-06-01.

[34] f b.no. Thief pretended to be ambulance driver. http://www.f-b.no/nyheter/tyv-utga-seg-for-a-vere-ambulansesjafor-1.7862440. Last Accessed: 2013-06-01.

[35] dagbladet.no. Disguised sex offender broke into prison. http://www.dagbladet.no/2013/03/04/nyheter/fengsel/usa/26044246/. Last Accessed: 2013-06-01.

[36] Hågen Hasle, Yngve Kristiansen, K. K. & Snekkenes, E. 2005. Measuring resistance to social engineering.

[37] Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. 2010. Experimental case studies for investigating e-banking phishing techniques and attack strategies.

[38] Yin, R. K. 2009. *Case Study Research - Design and Methods, Fourth Edition*. SAGE Publications, Inc.

[39] digi.no. Search more dangerous than porn. http://www.digi.no/912074/sok-er-farligere-enn-porno. Last Accessed 2013-04-12.

[40] Sikkerhetsråd, N. Morketallsundersokelsen-2010. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/morketallsundersokelsen_2010.pdf. Last Accessed: 2013-05-27.

[41] Jacobsen, D. I. 2005. *Hvordan gjennomføre undersøkelser - innføring i samfunnvitenskapelig metode*.

[42] Komiteer, F. For debatt om metoder og resultater. www.etikkom.no. Last Accessed: 2013-06-01.

[43] SANS, M. V. H. Targeted social engineering. http://isc.sans.edu/diary/Targeted+social+engineering/5707. Last Accessed: 2013-05-27.

[44] Yin, R. K. 2011. *Qualitative Research from Start to Finish*. The Guilford Press.

[45] Lacey, D. 2009. *Manaing the Human Factor in Information Security*. John Wiley & Sons Ltd,.

[46] wired.com. Evernote hack exposes user data, forces extensive password resets. http://www.wired.com/threatlevel/2013/03/evernote-hack-password-resets/. Last accessed: 2013-04-01.

[47] Janczewski, L. & Lingyan, F. 2010. Social engineering-based attacks: Model and new zealand perspective.

[48] NorCERT. 1st. quarterly report, 2012.

[49] NSM. What must you do to prevent employees from being victim of social engineering? http://blogg.nsm.stat.no/archives/3123. Last Accessed 2013-04-27.

[50] Enisa. 2007. Information security awareness initiatives: Current practice and the measurement of success.

[51] Prestaasen, B. Improving security awareness and ownership using a method based on action research,. Master's thesis, 2011. Last Accessed: 2012-08-26.

[52] Chelsa Russell, S. 2002. Security awareness - implementing an effective strategy.

[53] Rebecca Thurmond Fowler, S. 2007. Making security awareness efforts work for you.

[54] Lew McCreary, C. 2006. Security awareness programs: Now hear this!

[55] onguardonline.gov. 2012. Onguardonline. http://www.onguardonline.gov/media. Last Accessed: 2012-10-22.

[56] SANS. Securing the human, security awareness. https://www.securingthehuman.org/media/resources/pdfs/sec awareness-brochure.pdf. Last Accessed 2013-04-20.

A Appendix

TV-Series about Social Engineering

For those particularly interested in Social Engineering, below for your potential amusement, are several TV-series touching the topic.

Lie to Me

Dr. Cal Lightman teaches a course in body language and makes an honest fortune exploiting it. He's employed by various public authorities in various investigations, doing more when the police etc. fail to go the extra mile. So he can afford to constitute a team of his own, which like clients and others has to put up with his mind-games. (IMDB.com)

Burn Notice

A spy recently disavowed by the U.S. government uses his Special Ops training to help others in trouble. (IMDB.com)

White Collar

A white collar criminal agrees to help the FBI catch other white collar criminals using his expertise as an art and securities thief, counterfeiter and racketeer. (IMDB.com)

The Mentalist

An infamous 'psychic' abandons his public persona, outing himself as a fake, to focus on his work as a consultant for the California Bureau of Investigation in order to find "Red John," the madman who killed his wife and daughter. (IMDB.com)

The Real Hustle

A team of real-life confidence tricksters carry out notorious scams on unsuspecting members of the general public whilst hidden cameras capture all the action. (IMDB.com)

Request for Action, retrieved from The Art of Deception, Mitnick

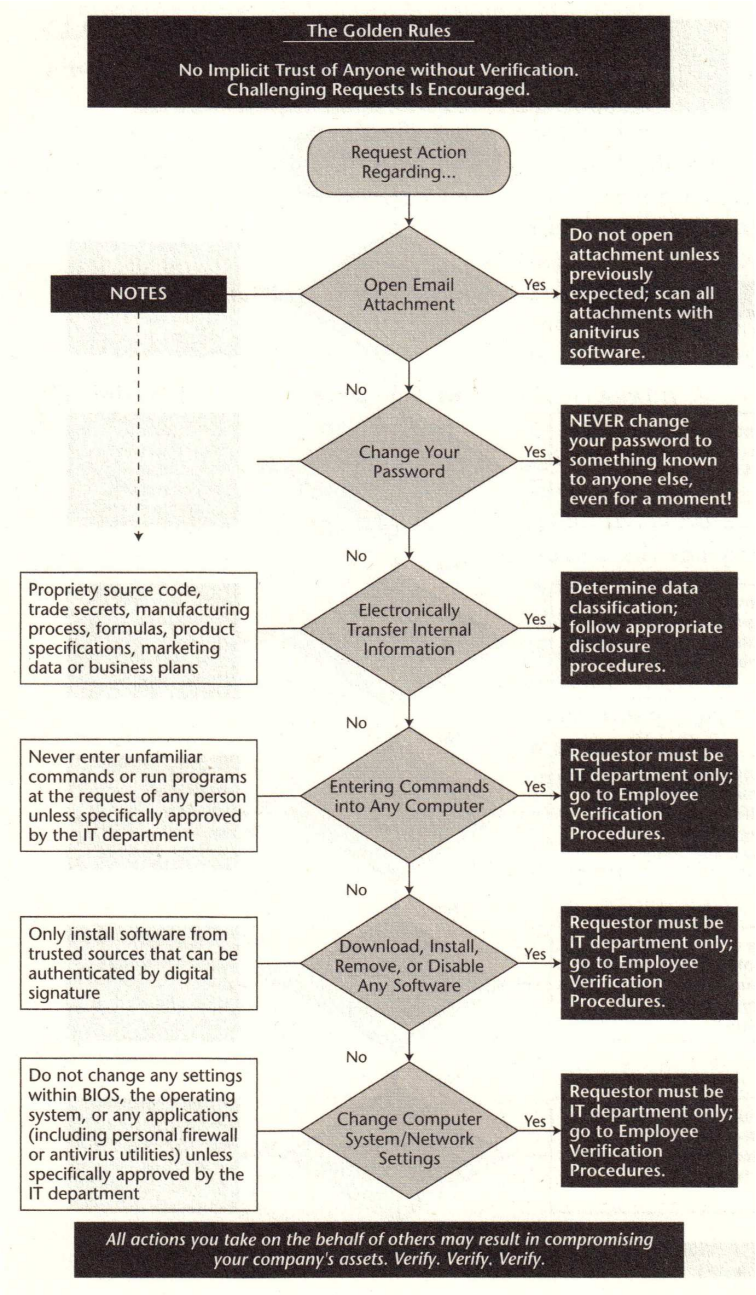

Figure 59: Request for Action, retrieved from The Art of Deception, Mitnick

Request for Information, retrieved from The Art of Deception, Mitnick

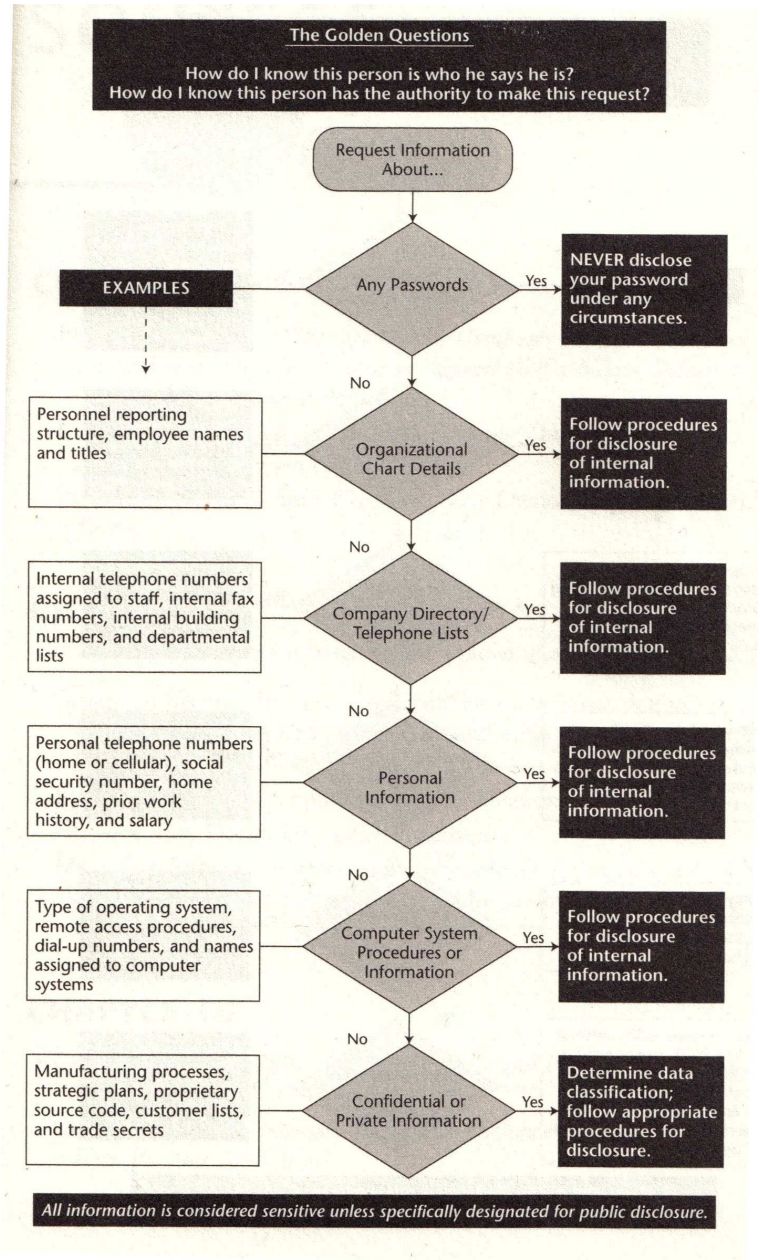

Figure 60: Request for Information, retrieved from The Art of Deception, Mitnick

Mitnick's Proposition of Verification

Verification of Identity Procedure

Called ID: Verify call is internal, and name or extension number matches the identity of the caller

Callback: Look up requester in company directory and call back the listed extension

Vouching: Ask a trusted employee to vouch for requester's identity

Shared common secret: Request enterprise-wide shared secret, such as a password or daily code

Supervisor or manager: Contact employee's immediate supervisor and request verification of identity and employment status

Secure email: Request a digitally signed message

Personal voice recognition: For a caller known to employee, validate by caller's voice

Dynamic passwords: Verify against a dynamic password solution such as Secure ID or other strong authentication device

In person: Require requester to appear in person with an employee badge or other identification

Verification of Employment Status Procedure

Employee directory check: Verify that requester is listed in on-line directory

Requester's manager verification: Call requester's manager using phone number listed in company directory

Requester's department or workgroup verification: Call requester's department or workgroup and determine that requester is still employed by company

Procedure to Determine Need to Know

Consult job title/workgroup/responsibilities list: Check published lists of which employees are entitled to specific classified information

Obtain authority from manager: Contact your manager, or the manager of the requester, for authority to comply with request

Obtain authority from the information Owner or designee: Ask owner of information if requester has a need to know

Obtain authority with an automated tool: Check proprietary software database for authorized personnel

Criteria for Verifying Non-Employees

Relationship: Verify that requester's firm has a vendor, strategic partner, or other appropriate relationship

Identity: Verify requester's identity and employment status at the vendor/partner firm

Nondisclosure: Verify that the requester has a signed nondisclosure agreement on file

Access: Refer the request to management when the information is classified above Internal

Master Thesis: Defending against Social Engineering - Questionnaire

Your identity will be hidden.
Read more about confidentiality and hidden identity here. (Opens in a new window.)

Dear Sir or Madam,

Thanks for your initial effort on accessing this Questionnaire about Social Engineering.

Within the boundaries of this Questionnaire we define "Social Engineering" (SE) as:

" A request with the intention of getting unauthorised access to information and/or services, typically by manipulating the requested to believe that the requester is someone else than he/she really is".

For all questions; please consider events that has occurred **since the 1st of January 2011 and later**.

All answers are anonymous.

- Thanks again!

1) What type of Organization do you represent? (You can choose how specific you want to be - leave it blank if you don't want to say)

2) * How many employees does your Organization consist of? (of which you can represent for the purpose of this Questionnaire)

Select answer

Next >>

20 % completed

Master Thesis: Defending against Social Engineering - Questionnaire

TARGETED / NON-TARGETED ATTACKS

The questions on this page regards Social Engineering attacks that are considered to be NON-TARGETED or TARGETED.

Non-targeted attacks is general queries sent to many people/Organizations, for instance telling that they are from Microsoft Helpdesk and need you to install some software. They usually don't have any information that regards "you" in their request.

In contradiction, TARGETED attacks could be the same query, but aimed/tailored towards a few individuals. A targeted attack often use information that are in some way tied to you, or those around you, like your name, birthdate, phonenumber,job-position etc. (ex. Spear Phishing)

If an identical request is "sent" to several employees of an Organization, within a limited time period, it should for the purpose of this Questionnaire be considered as -one- incident.

Daily advertisement (SPAM) should not be included.

NON-Targeted Attacks

4) * How many times have your Organization experienced NON-targeted Social Engineering attacks?

	None	1-2	3-5	6-10	11-20	21-50	51-100	100++	I don't know	No Comment
By E-Mail:	○	○	○	○	○	○	○	○	○	○
By Physical Mail:	○	○	○	○	○	○	○	○	○	○
By SMS:	○	○	○	○	○	○	○	○	○	○
By Phone:	○	○	○	○	○	○	○	○	○	○
By Adversary showing up in person:	○	○	○	○	○	○	○	○	○	○
By using Social Networks, like Facebook:	○	○	○	○	○	○	○	○	○	○
By surfing on websites	○	○	○	○	○	○	○	○	○	○

Targeted Attacks

5) * How many times have your Organization experienced TARGETED Social Engineering attacks?

	None	1-2	3-5	6-10	11-20	21-50	51-100	100++	I don't know	No Comment
By E-Mail:	○	○	○	○	○	○	○	○	○	○
By Physical Mail:	○	○	○	○	○	○	○	○	○	○
By SMS:	○	○	○	○	○	○	○	○	○	○
By Phone:	○	○	○	○	○	○	○	○	○	○
By Adversary showing up in person:	○	○	○	○	○	○	○	○	○	○
By using Social Networks, like Facebook:	○	○	○	○	○	○	○	○	○	○
By surfing on websites	○	○	○	○	○	○	○	○	○	○

6) In regard to the attacks you have experienced, if any; are you able to say some words about what happened?

"Information about Incident here" / "No Comment"

<< Back Next >>

40 % completed

Master Thesis: Defending against Social Engineering - Questionnaire

SUCCESSFUL ATTACKS

On this page we will focus on questions regarding successful attacks. We define successful attacks as attacks where the "victim" has accepted the adversary's query. This could for instance be to let a person in to the building, or click on a certain link in an email.

Please note that whether or not your Organization suffered loss from this incident, IS NOT relevant when answering the questions on this page.

Successful, NON-Targeted Attacks

8) * How many times have you experienced SUCCESSFUL, NON-TARGETED Social Engineering attacks?

	None	1-2	3-5	6-10	11-20	21-50	51-100	100++	I don't know	No Comment
By E-Mail:	○	○	○	○	○	○	○	○	○	○
By Physical Mail:	○	○	○	○	○	○	○	○	○	○
By SMS:	○	○	○	○	○	○	○	○	○	○
By Phone:	○	○	○	○	○	○	○	○	○	○
By Adversary showing up in person:	○	○	○	○	○	○	○	○	○	○
By using Social Networks, like Facebook:	○	○	○	○	○	○	○	○	○	○
By surfing on websites	○	○	○	○	○	○	○	○	○	○

Successful, Targeted Attacks

9) * How many times have you experienced SUCCESSFUL, TARGETED Social Engineering attacks?

	None	1-2	3-5	6-10	11-20	21-50	51-100	100++	I don't know	No Comment
By E-Mail:	○	○	○	○	○	○	○	○	○	○
By Physical Mail:	○	○	○	○	○	○	○	○	○	○
By SMS:	○	○	○	○	○	○	○	○	○	○
By Phone:	○	○	○	○	○	○	○	○	○	○

By Adversary showing up in person:	○	○	○	○	○	○	○	○	○	○
By using Social Networks, like Facebook:	○	○	○	○	○	○	○	○	○	○
By surfing on websites	○	○	○	○	○	○	○	○	○	○

10) In regard to the successful attacks you have experienced, if any; are you able to say some words about what happened?

"Information about Incident here" / "No Comment"

11) * If Successful attacks, what do you estimate your economic losses to be because of it? (In NOK)

Select answer

<< Back Next >>

60 % completed

Master Thesis: Defending against Social Engineering - Questionnaire

DEFENSE MECHANISMS

On this page we will focus on questions regarding your DEFENSE MECHANISMS against Social Engineering. This could for instance be certain procedures that are set in motion when people call to your Organization (ex. verifying the identify of the caller by codewords), or Security Awareness programs that employees needs to attend yearly.

13) Do you currently have Defense Mechanisms in place to counter Social Engineering attacks?

Yes No No Comment I don't know

14) Are you planning on implementing (more) Defense Mechanisms to counter Social Engineering attacks?

Yes No No Comment I don't know

15) Do you think/know that you have countered an Social Engineering attack because of having Defense Mechanisms?

Yes No No Comment I don't know

<< Back Next >>

80 % completed

Master Thesis: Defending against Social Engineering - Questionnaire

ELABORATING

On this page we will focus on elaborating on the questions you answered on the previous page.

This box is shown in preview only.

The following criteria must be fulfilled for this question to be shown:

- (
  - If "Do you currently have Defense Mechanisms in place to counter Social Engineering attacks?" *equals* "Yes"
-)

17) Can you elaborate on what Defense Mechanisms you have in place to counter Social Engineering? (Detection/Prevention/Correction)

"Elaborate here" / "No Comment"

This box is shown in preview only.

The following criteria must be fulfilled for this question to be shown:

- (
  - If "Do you currently have Defense Mechanisms in place to counter Social Engineering attacks?" *equals* "No"
-)

18) Can you say anything about -why- you have no Defense Mechanisms in place to counter Social Engineering?

"Elaborate here" / "No Comment"

This box is shown in preview only.

The following criteria must be fulfilled for this question to be shown:

- (
  - If "Are you planning on implementing (more) Defense Mechanisms to counter Social Engineering attacks?" *equals* "Yes"
-)

19) Can you elaborate on what Defense Mechanisms you plan to implement to counter Social Engineering? (Detection/Prevention/Correction)

"Elaborate here" / "No Comment"

This box is shown in preview only.

The following criteria must be fulfilled for this question to be shown:

- (
  - If "Are you planning on implementing (more) Defense Mechanisms to counter Social Engineering attacks?" *equals* "No"
-)

20) Can you say anything about -why- you are not implementing (more) Defense Mechanisms to counter Social Engineering?

"Elaborate here" / "No Comment"

This box is shown in preview only.

The following criteria must be fulfilled for this question to be shown:

- (
  - If "Do you think/know that you have countered an Social Engineering attack because of having Defense Mechanisms?" *equals* "Yes"
-)

21) Can you elaborate on your Successful defense(s) of a Social Engineering attack?

"Elaborate here" / "No Comment"

22) * How big of a security risk do you consider Social Engineering to be towards your Organization?

Very Low Low Medium High Very High I don't know No Comment

<< Back Send

100 % completed