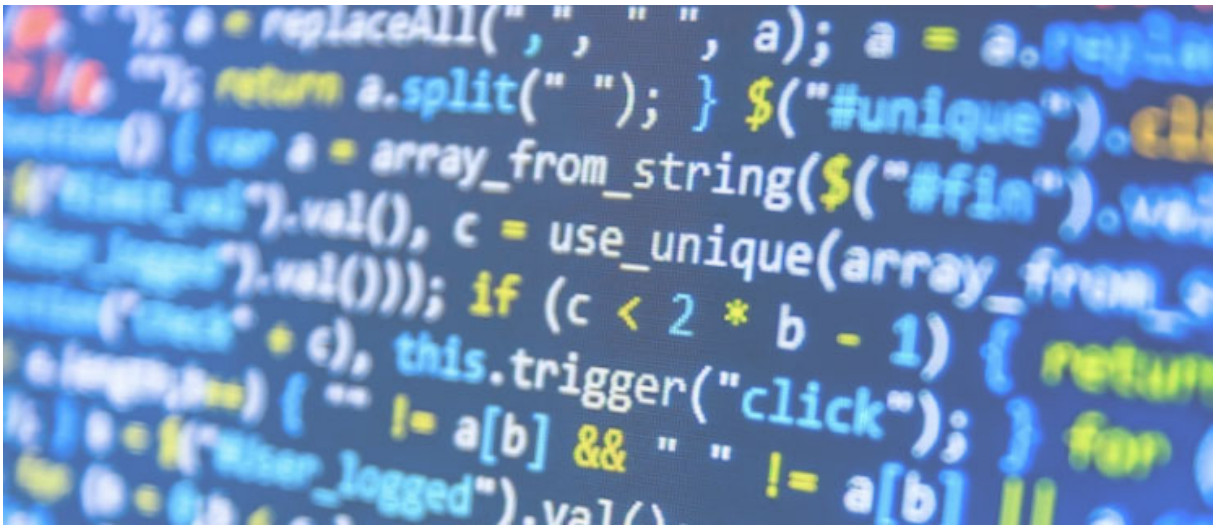
A methodology for quantifying the level of cybersecurity awareness



Robert de Vries
S1789899

Master Thesis
Executive Master in Cyber Security

Supervisors
Prof. dr. Jan van den Berg
Mr. Sergei Boeke
Drs. Xander van der Voort

Leiden University
Faculty of Governance and Global Affairs
Cyber Security Academy, The Hague

Leidschendam, 7 December 2017

Acknowledgement

To my beloved wife, my tower of strength: because my heart is yours. I owe you my unconditional love.

The past few months must have been hard for you, as all my spare time was devoted to this thesis. Without any hesitation, I had your complete support. You tore me away when my thesis looked like a Groundhog Day. You gave me inspiration when I was completely stuck and you always were strict to me when I had to take a coffee break.

I am grateful to the Royal Netherlands Marechaussee (RNM), which agreed I could use the data from the case study. I am also grateful to Edwin, who believed in me even though he was not my direct chef. Special thanks go to all employees who thought they would get an iPhone, were disappointed they eventually didn't, but saw through the necessity of deception. I even would like to thank those employees who got mad and filed reports in my name, as even they have become part of my thesis. In addition, I would like to thank KiXS and Charlotte in particular for their hard work in providing the technical solution and conducting the phishing experiment.

I would like to thank all my fellow students who were nice enough to be interviewed as specialists, and all specialist experts which gave me interesting insights into their organizations.

A very special gratitude goes to my university supervisors: Jan, Sergei and Xander, who were my scientific conscience, supported me and gave me inspiring feedback.

Last but certainly not least, I would like to thank my parents, my parents in law, my brother and my brothers and sisters-in-law. You are my family and I am grateful to be part of it.

I would like to end with the famous words from *Sir Francis Bacon, Ipsa scientia potestas est*, but I would like to add my own twist, nihil verberat familia.

Abstract

According to the yearly publication of Dutch National Cyber Security Center of the current cyber security situation of the country (Cyber Security Beeld Nederland -CSBN- 2017) a cyber-attack originated in 91% of the investigated cases from some form of phishing. This is in line with data from the SysAdmin, Audit, Network and Security (SANS) institute that states: *'95% of all attacks on enterprise networks are the result of successful spear phishing.'* Because a very high percentage of cybersecurity incidents start with some kind of phishing, the action and reaction of employees on phishing attacks could be used as a measurement method to quantify the level of cybersecurity awareness (CSA) of an organization.

Governmental organizations invest millions in the protection of their internal systems and infrastructure, but only train their employees in a low-cost, short duration, Cybersecurity Awareness (CSA) course. There are huge investments in defensive technologies, but little investments in human awareness. Quantifying the level of awareness of employees can be used to measure changes in the level of CSA of that particular organization. Some methodologies to quantify the level of CSA are available, but these methods are scarce and sometimes inconsistent.

This thesis researches the available CSA-level measurement methods and proposes a methodology based on quantification of the factual measurement level of cybersecurity awareness of organizations. The methodology finds its foundation in literature, expert interviews and a case study in which gamification of a phishing attack was studied.

Data from a case study performed within the Dutch Ministry of Defense is examined, in order to explain why gamification can be used as a CSA-level measurement method and/or why gamification can be used as supplement or validation method of existing methods. Phishing is used as gamification method. A distinction is made between phishing and spear phishing. Using the optional 'Vishwas' triad and psychological influence factors, a differentiation in phishing methods can be used in quantification methods. To create validated findings, the gamification research has to be conducted in a scientific manner, with an appropriate research design, defining the minimum target population, selecting a proper sampling scheme and by collecting the data in a secure and privacy preserving manner.

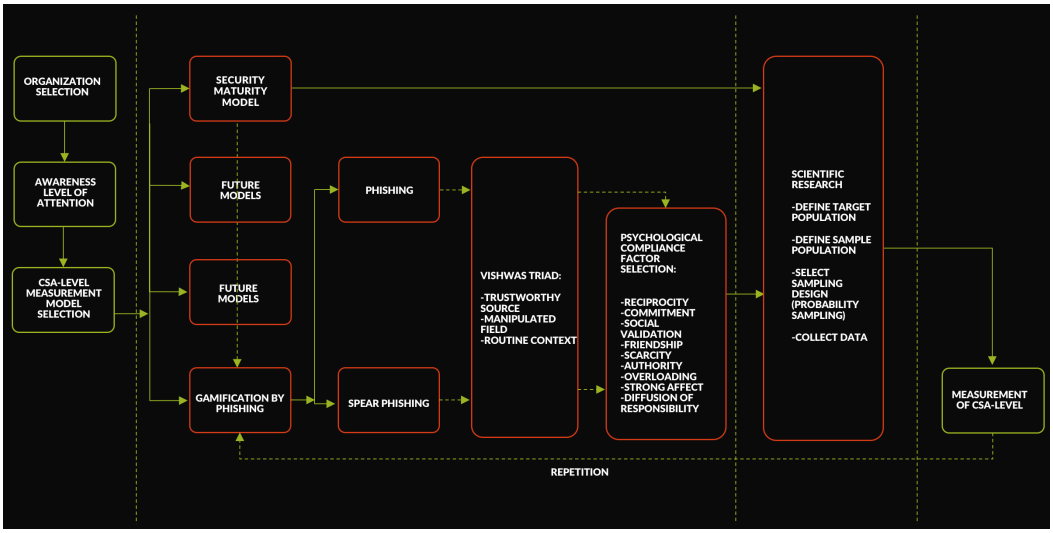


Table of Contents

“Sometimes, it is easier to hack the human firewall, than to hack the computer firewall.”
Steven Wilson, Head of European Cybercrime Centre (2017)

1 Introduction

1.1 Motivation

According to the yearly publication of Dutch National Cyber Security Center of the current cyber security situation of the country (NCSC, 2017) a cyber-attack originated in 91% of the investigated cases from some form of phishing. This is in line with data from the SANS institute: '*95% of all attacks on enterprise networks are the result of successful spear phishing* (Brecht 2015)*.'* Therefore, quantifying how employees react on a phishing exercises can give an indication of their awareness of cybersecurity. Due to the fact that a very high percentage of cybersecurity incidents start with some kind of phishing, the action and reaction of employees on phishing attacks could be used as a form of measurement method to quantify the level of Cybersecurity Awareness (CSA) of an organization.

Governmental organizations invest millions in the protection of their internal systems and infrastructure, but often train their employees in a low-cost short duration CSA course (SANS 2016b). There are huge investments in defensive technologies, but little investments in human awareness. Although employees are a very important resource for the organization and play an important role in cybersecurity, they can also be the weakest link in cybersecurity (Norrie Johnston Recruitment 2017). Therefore, organizations need to mitigate this 'weakest link' by giving their employees situational awareness in cybersecurity. This not only makes them aware of the threats, but cybersecurity aware personnel also can act as cybersecurity sensors in their organization and can become the strongest link in the overall cybersecurity effort.

Generally, there are two approaches of quantifying CSA (SANS 2016a). The first approach is to research the existence of an awareness program in an organization and subsequently quantifying the maturity of this program. The second approach is quantifying the effect of the awareness training on the actual behavior of the trainees. In order to achieve effective cyber security management, CSA training and a cybersecurity strategy are necessary (Belaissaoui & Elkhannoubi 2015). Cybersecurity partially can be achieved by training the employees. Not only is it important to quantify the maturity level of a CSA training program of an organization, but it is equally important to measure the effect of training on the behavior of the employees. Since the actual behavior of employees defines to what extent they are deteriorating cybersecurity, the focus of this thesis is on quantifying the effect on the actual behavior of employees that have had an awareness training.

Two methods to measure the effect on the behavior of employees of the awareness training have been found. The first method is the Kruger & Kearney method (K&K-method), which uses surveys in combination with models from social psychology to measure and analyze attitude, knowledge and behavior of employees in several focus areas, each with its own weighting criteria (Kruger & Kearney 2006). The second method, which is based on the K&K-method, is the Human Aspect of Information Security Questionnaire (HAIS-Q) (Parsons, McCormac, Pattinson, et al. 2014). The HAIS-Q method also uses standardized questionnaires in several focus areas to measure attitude, knowledge and behavior of employees, but doesn't use added weighting criteria for their focus areas (Parsons, McCormac, Pattinson, et al. 2014).

The HAIS-Q method and the K&K method are based on questionnaires or surveys, of which Kruger & Kearney already stated that the results of these possible suffer from being answered in a social desirable manner and thus may not be a very truthful reflection of reality (Kruger & Kearney 2006). The data found is dependent on what the respondents explain when completing the questionnaires or surveys, with the possibility of being based on subjective experience rather than facts. In this case, the responses may be subjective, as there is a high possibility of being the desirable answer, therefore questions may be asked about the validity of this method. As there are no other generally accepted measurement methods found in literature, a knowledge gap in available literature to measure actual behavior of employees (as opposed to social desirable answers to surveys) in cybersecurity is identified.

1.2 Research questions

The starting point for this thesis is the gap in the body of knowledge in the literature on measuring the level of CSA in organizations. *Therefore, the goal of this thesis is to develop a methodology for quantifying the level of cybersecurity awareness of organizations.*

Before developing a methodology to quantify the level of CSA of organizations, a better understanding of the role of CSA for cybersecurity is needed:

1a) What is the role of cybersecurity awareness for cybersecurity?

In chapter 2, this question is answered by looking deeper at behavioral aspects of cybersecurity. Looking at different behavioral points of view in relation to cybersecurity and CSA will aid in developing fining a new methodology to quantify the level of CSA. This leads to the following research question:

1b) What are the elements that determine the CSA levels of an organization?

The answers on this question are described in chapter 2, and can be used to create a body of understanding on what should be measured in order to quantify the level of CSA of organizations. Understanding of elements that determine the CSA level is needed to assess current methods to quantify the level of CSA. This understanding lead to the following research question:

2) Which methods are available to determine the level of cybersecurity awareness of an organization?

Available methods are described in chapter 3 and compared to each other. After providing information on available methods of quantifying the level of CSA, these methods are examined for usefulness and validity. Also gaps in the body of knowledge will be presented, in order to validate the goal of this thesis.

3) Can gamification of phishing be used as a methodology for quantifying the CSA-level of an organization?

A case study which was designed and performed at the Royal Netherland Marechaussee (RNM) is described in chapter 4. As the case study uses a gamification of spear phishing, the results of this case study will be compared to existing CSA-level measurement methods described in chapter 3. In chapter 4 requirements are determined which are used as input for the methodology design in chapter 5. At the end of chapter 5, as validation some expert opinion is given on the practicality and usability of the new proposed methodology.

Chapter 4 describes a case study which was performed at the RNM. As the case study is a gamification of spear phishing, the results of this case study will be compared to existing CSA-level measurement methods described in chapter 3. Next, elements that can be used in the development of a new methodology on data driven measurement for measuring the level of CSA will be derived from the case study and used in chapter 5. The first part of chapter 4 describes the setup of the case study and the lessons learned from the case study. The case study is an integral part of the research. Combined with the literature study and expert-interviews from chapter 2 and chapter 3 it is used to reach the research goal. The second part of chapter 4 describes results and analysis of these results of this case study. Chapter 4 concludes with an overview of elements and helpful lessons learned which can be used for measurement of CSA-levels.

1.3 Research methodology

In order to answer the research questions, multiple methods of research have been used. This paragraph explains which research methods were used in this thesis and why these were chosen. In this thesis, literature study, online research, semi-structure experts' interviews and a case study have been used to perform research. First, the reasoning behind using the methods and secondly, the manner in which they were executed is explained. Next, an overview will be given in which chapters these methods were used:

- A literature study was done to find information on the topics of this thesis. The Leiden University online library was used to find recent information on the thesis topics.
- Online research was used to correlate literature found with recent information published by specialized companies. Due to their position in the cybersecurity landscape these companies will most likely have very up-to-date information.
- Semi-structured interviews with field-experts related to the Ministry of Defense (MoD) were performed. These experts were chosen, because they were easily accessible and all have some relation to the security of the Netherlands. Semi-structured interviews were specifically chosen, because the field-expert could tell their own story in which the subjects could be told in no specific order. The field-experts were told the subject and direction of the interview in advance. During the interviews, the topic of the thesis was presented and related to the questions. Minutes from the interviews were recorded.
- Data from a case study was collected and enriched with additional data. This data was saved in an Excel spreadsheet data file, so it could be used for data analysis.
- Design science was applied and the collected data was analyzed. Design science is focused on the performance and development of requirements and was chosen to develop a new improved methodology. In the reflection of chapter 5 the practicality and usability of the proposed methodology was validated by field experts.

Chapter 2, describes the results of a literature study that was done to collect information and perform comparative research on the role of CSA for cybersecurity. Elements that determine the level of CSA of an organization are defined. The Leiden University online library was used to find recent information on cybersecurity and CSA related topics in relation to behavior of people. Some publications were found, however because cybersecurity and therefore CSA and its essential elements are continuously under development and therefore evolving topics, additional online research and semi-structured interviews with field-experts in the Netherlands were performed to validate the information found in the literature or to update this information. This online research and interviews were used to triangulate and augment the found information in the literature study.

Chapter 3, describes the results of a literature study that was done to collect information and to perform a comparison of available methods to determine the level of CSA of an organization. The Leiden University online library was used to find recent information on available methods, specifically focused on human behavior in comparison with the level of CSA. Also, semi-structured interviews were used in order to determine if field-experts already used some sort of measurement method. Next, an analysis of the limitations of available methods was performed, in order to find a gap in the body of knowledge on these available methods.

In chapter 4 two case studies are presented, of which case study 1 was performed by us before the start of this thesis. Only after completing this study, its results were assessed as valuable input for this thesis. Specifically, for this thesis, all collected data was put in an Excel spreadsheet data file in order to be analyzed more thoroughly using quantitative methods. Case study 1 consists of a phishing experiment, in which three groups were sent phishing emails of which the results were collected. Case study 2 was performed specifically for this thesis, in which additional information, by use of a questionnaire, was asked to all participants of phase 1. Unfortunately, not all participants of case study 1 reacted in the questionnaire of case study 2. The lessons learned in the performed case study are used to identify a possible solution for the knowledge gap in the literature on measuring the effectives of CSA programs. The results of case study 2 were also put in the Excel spreadsheet data file. Because the phishing experiment was only meant as a proof of concept within the MoD, the resulting experimental design did not provide for independent, randomly assigned treatment groups. Therefore, no scientific conclusions can be made from this experiment. However, the results seem to provide a trend which was also found in other research and therefore provide interesting directions for additional research, of which some results are also presented in chapter 4.

In chapter 5, results of the literature study, online research, semi-structured interviews and case study are used to design a new methodology to quantify the level of CSA.

Figure 1: research model

In chapter 6 the conclusion of the thesis will be presented. The bibliography is presented in chapter 7. Information on the case study and experts interviewed can be found in Appendix A. Due to the sensitive nature of some interviews, minutes of the conducted interviews are not admitted to the Appendix. A sample of the dataset is given in Appendix B.

The research model (figure 1) gives a helicopter view of the structure of this thesis and displays the building blocks used in this thesis, in order to design a methodology to quantify the level of CSA. All chapters begin with a description of the purpose of the chapter, the approach used and end with a conclusion.

1.4 Limitations of research

This thesis also has some limitations. In total eight field-experts were consulted, of seven of which were Dutch and related to the MoD and one was American and an expert in phishing experiments. Some information provided in the interviews was confidential and not to be disclosed and only general information has been used for statistical purposes. There is also a possibility information derived from these interviews were personal opinions of these field-experts in contrast with the actual 'company viewpoint'. Although the interviewer performed the interviews as a student of the Cyber Security Academy, he was also employee of the MoD at that time. Because the interviewees were aware of this, there always is a possibility the information given is biased. Although the performed interviews show similarities in answers, no fact checking was performed with other sources from the same organizations.

As mentioned earlier, the performed case study was not designed for this thesis, only the second case study was. What is more, the investigated group were all employed at the Royal Netherlands Marechaussee. There is a possibility the results from this group will not be generalizable when conducted at another organization.

1.5 Structure of thesis

CHAPTER	TITLE	DESCRIPTION
1	Introduction	Presenting the background, motivation, problem statement, research questions, methodology and structure of the thesis.
2	Cybersecurity and the role of cybersecurity awareness	Presenting insight into cybersecurity and the role of cybersecurity awareness by providing background information, such as the relation to human behavior, social engineering and spear phishing, psychological aspects and existing training programs.

3	Existing models on quantifying CSA-levels.	Description of existing models on quantifying CSA-levels, assessment of these models and presenting the knowledge gap in current literature.
4	Case studies	Presentation of case study 1 and case study 2 of the performed case study. Identification of lessons learned and presentation of possible solution for knowledge gap.
5	Design of measurement methodology	Validation of new design through findings of literature and case studies. Proposal of new approach to quantify the level of cybersecurity awareness.
6	Conclusion & recommendations	Thesis conclusion and summary of the findings, proposal, conclusions and recommendations of the thesis.
7	Bibliography	Literature used.
	Appendixes	
A	Research accountability	Accountability of conducted literature study, interviews and case studies.
B	Dataset example	Example and explanation of the used dataset.

Table 1: Structure of thesis

2 Cybersecurity and the role of cybersecurity awareness

2.1 Introduction

This chapter describes the role of CSA in cybersecurity and the elements that determine the CSA levels of organizations. First an introduction to cybersecurity is given, in which a distinction is made between traditional information security and cybersecurity. However, the focus of this thesis will be on behavioral aspects of cybersecurity and CSA. These behavioral aspects will be connected to social engineering and spear phishing. A more in-depth view will be given on the psychological aspects of cybersecurity as these aspects can be used in the conceptualization of a new methodology. Then, behavioral and psychological related aspects found will be related to existing training programs. This chapter finalizes with an overview of identified issues. These identified issues will be used in the design of the new measurement methodology in chapter 5.

2.2 Information security vs cybersecurity

Before explaining what cybersecurity is, it is important to compare cybersecurity with the more generally known concept of information security. In general it is recognized that information security and cybersecurity are often used interchangeably in an unstructured manner (van den Berg 2015). Although this is not desirable, this can be explained, because the term information security describes: '*the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption* (SANS n.d.)*'.* Although this definition has some similarity with cybersecurity, cybersecurity itself goes one step further, by redefining cyberspace (van den Berg 2015). Where information security is more technically focused, cyberspace adds two additional layers, the socio-technical layer in which the technology has to be controlled by humans, and the governance layer, in which the cyber aspect has to be incorporated in the strategic processes of the organization. This resulted in the 3-layer cyberspace model:

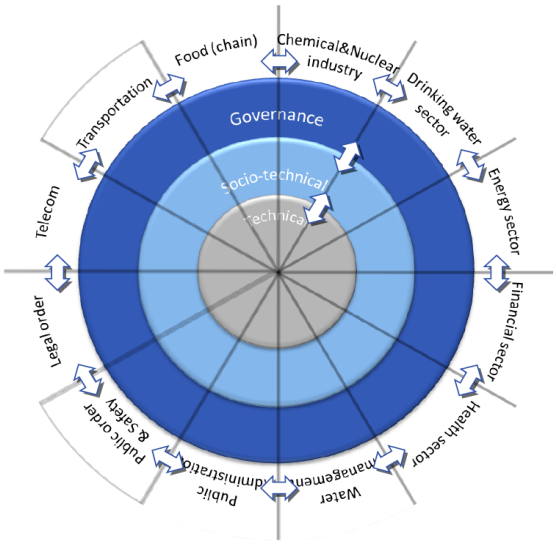


Figure 2: 3-layer cyberspace model (van den Berg 2015, p 4-5)

The technical layer (grey colored center layer) incorporates the old view of information security, and provides the possibility of cyber activities. The socio-technical layer connects technology with human interaction. Cyberspace incorporates all cyber activities and needs governance, so the model concludes with the governance layer.

The problem however, is that information security awareness programs are often focused on the technical layer and designed to let employees (Wilson et al. 2003):

- Learn their part and duty as part of the mission of the organization;
- Learn and understand the security policies, procedure and processes of the organization;
- Learn know-how of numerous disciplines (from management-, operational- and technical perspective) which are needed to take care of IT.

Because information is now connected to cyberspace, information cannot be secured in the technical layer only. This human behavior in executing cyber activities, which result in human (in)actions now not only takes place in the technical layer, but also in the socio-technical layer and form an additional threat in cybersecurity now. The three-layer model of van den Berg sees humans using IT as the weakest link in cybersecurity.

Only in the last few years are cybersecurity programs evolving to incorporate the socio-technical layer. To rationally govern the level of cybersecurity awareness within an organization it is necessary to have factual measurable indicators for awareness. Although some information and cybersecurity awareness quantifying methods are available, these methods are not standardized and adopted by normative organizations.

Previous CSA training was more focused on information security (technical layer) (van den Berg 2015). This thesis is focused on human behavior in cyberspace, which can be trained with CSA programs. Therefore, this thesis focusses on the socio-technical layer of cyberspace, the layer of cyberspace in which technology and people interact with each other (van den Berg 2015) and in which human actions and inactions, the cyber-activities can be misused.

In order to mitigate the risk of employees performing an insecure action, organizations use various compliance methods, like having rules, regulations but also by training their employees to increase their level of awareness. In this case, this thesis focuses on awareness around cyber-activities. Although having cybersecurity awareness processes for compliancy purposes are important, human behavior can contribute to the safety and security of the organization, in other words to the resilience of the organization (Grøtan 2014). Instead of viewing human behavior as a disadvantage (as they can become a liability), it is now seen as a resource, for example because all your employees now are sensors. This viewpoint requires a bottom-up approach from the organization in which the employees need to be actively trained.

2.3 Cyber (in)security

The previous paragraph explained the difference between information security and cybersecurity. As this thesis focuses on cybersecurity, it is essential to explain what cybersecurity encompasses. In literature, there is no one exact definition of what

cybersecurity entails. Moreover, there is no general understanding on how to write cybersecurity. There is no general understanding within companies. For example, a well-known cybersecurity company Fox-IT uses: 'Cyber Security', 'Cyber security', 'cyber security', 'Cybersecurity' and 'cybersecurity' on its own webpage (Fox-IT 2017). In this thesis 'cybersecurity' is chosen. When trying to find a definition in publications, it seems like it is assumed the definition of cybersecurity is common knowledge. The complication of cybersecurity is, it is a term which is used as comprehensive understanding, which makes it very difficult to generalize a common definition.

Table 2 below gives an overview of recent definitions used by standardization organizations ISO and NIST, the definition used by the cybersecurity center of the Netherlands (NCSC)and the definition used by the Cyber Security Academy (Cyber Security Academy 2017). Not only was this last definition added, because of the obvious relationship with the university, but also because the ABDO 2017 (Algemene Beveiligingseisen Defensie Opdrachten, (Ministry of Defense 2017)), to which all Dutch organizations which want to do business with the MoD have to comply, refers to the glossary of the Cyber Security Academy. In paragraph 2.2 the difference between information security and cybersecurity was described, by making use of the 3-layer cyberspace model of van den Berg. It is remarkable to note the definition of cybersecurity, taken from the website the Cyber Security Academy appears to be more focused on information security, like ISO/IEC 27000:2016 and NIST, in contrast to the 3-layer cyberspace model of van den Berg which focuses on securing human cyber-activities in cyberspace. The latter is used in this thesis.

USED BY	YEAR	DEFINITION USED
ISO/IEC 27000:2016	2016	*"Information security ensures the confidentiality, availability and integrity of information (ISO 2016)".*
NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY	January 2017	*"Cybersecurity's primary role is the preservation of the businesses value through the protection of the confidentiality, integrity, and availability (CIA) of the organization's information, operations, and processes (NIST 2017)".*
NATIONAL CYBER SECURITY CENTER (CYBER SECURITY ASSESSMENT NETHERLANDS 2016)	2016	*"The state of being free of danger or damage caused by a disruption or failure of IT or through the abuse of IT. The danger or damage caused by abuse, disruption or failure may comprise a limitation of the availability and reliability of the IT, violation of the*

		confidentiality of information stored in IT environments or damage to the integrity of that information (National Cyber Security Centre 2016)".
CYBER SECURITY ACADEMY NETHERLANDS	2017	*"Being free from danger or damage caused by disturbance or loss of ICT or abuse of ICT. The danger or damage caused by abuse, disturbance or failure may consist of limiting the availability and reliability of the ICT, violation of the confidentiality of information stored in ICT or damage to the integrity of that information (Cyber Security Academy 2017)".*

Table 2: overview of cybersecurity definitions

In addition, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has an overview of definitions from 35 countries. Not one is the same (CCDCOE 2017). The minimum general opinion of cybersecurity is that it has something to do with Confidentiality, Integrity and Availability (CIA). However, it is so much more. Figure 3, developed by the European Union Agency for Network and Information Security (ENISA), displays all aspects which can have effect on the definition of cybersecurity used by an organization (ENISA 2015), which shows CIA is a small part of the definition.

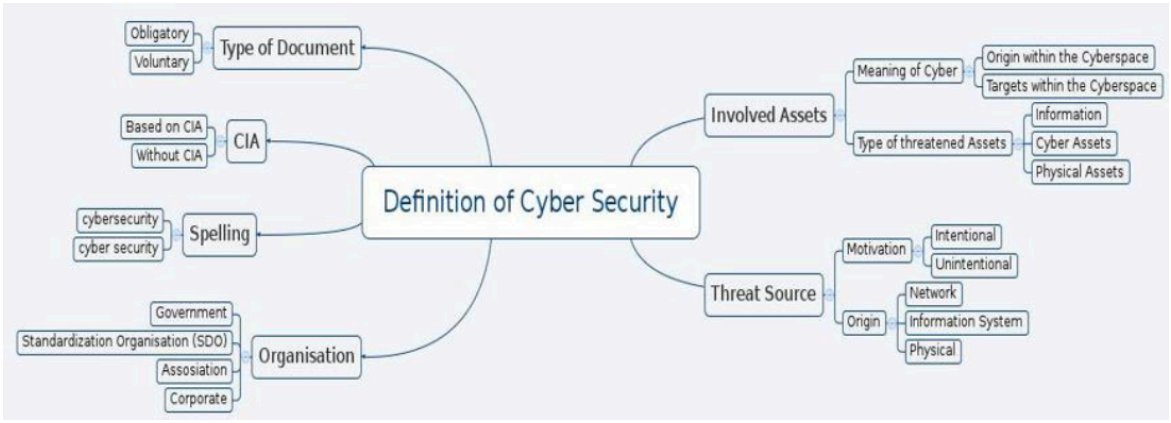


Figure 3: Components constituting the definition of Cybersecurity (ENISA 2015)

Although people agree cybersecurity is more than information security, the definitions used are still too much focused on the technical layer (CIA) (van den Berg et al. 2014). Besides technology driven security such as application security, information security, network security and IT-security a very important aspect of cybersecurity is awareness of users controlling the IT (ENISA 2016).

It becomes clear the word 'cyber' is the most misused word in combination with information security[1,2]. Cybersecurity consists of a combination of two parts, information security (CIA) with a more top-down corporate focus and a scope in the direction of the security of systems, processes and data (ISO 27001). Governments, vital infrastructures, organizations but also households are increasingly dependent on IT systems[3,4]. When CIA cannot be guaranteed anymore, any breach will have a bigger impact[5,6,7] . Because the impact of a breach in CIA can be enormous and not only relates to IT itself, cybersecurity adds the necessity to become part of an integral security plan, not only for governments, but even for households (Commision on enhancing national cybersecurity 2016).

Secondly, cybersecurity needs to be a top-priority at board level and has to have a more broad focus, in which the focus also is directed to the human aspect and the way processes are governed[8,9,10] (Ministry of Defense 2017). Besides having technical controls, also business continuity management, awareness and human behavior of IT has to be taken into account[11].

Cyber insecurity is the opposite of cyber security. However, there are also unknown unknowns, which means on top of security not being in place, it is also unknown what is unsecure and needs to be protected[12]. When cybersecurity aspects are not governed there may be a blind spot. Besides general applicable blind spots in cybersecurity a low cybersecurity maturity and not knowing the level of awareness of your employees is also cyber insecurity[13]. It is essential that the need for cybersecurity is accepted by the board and is the responsibility of everybody (bottom-up)[14].

[1] Vital Infrastructure Company 2 (2017) Interview on cybersecurity [Personal interview]

[2] Advisor DefCERT (2017) Interview on cybersecurity [Personal interview]

[3] Security Company 2 (2017) Interview on cybersecurity [Personal interview]

[4] Advisor CIO Office MoD (2017) Interview on cybersecurity [Personal interview]

[5] Advisor DefCERT (2017) Interview on cybersecurity [Personal interview]

[6] Security Company 2 (2017) Interview on cybersecurity [Personal interview]

[7] Advisor CIO Office MoD (2017) Interview on cybersecurity [Personal interview]

[8] Security Company 2 (2017) Interview on cybersecurity [Personal interview]

[9] Advisor CIO Office MoD (2017) Interview on cybersecurity [Personal interview]

[10] Vital Infrastructure Company 3. (2017) Interview on cybersecurity [Personal interview]

[11] Advisor DefCERT (2017) Interview on cybersecurity [Personal interview]

[12] Security Company 2 (2017) Interview on cybersecurity [Personal interview]

[13] Vital Infrastructure Company 3. (2017) Interview on cybersecurity [Personal interview]

[14] Security Company 2 (2017) Interview on cybersecurity [Personal interview]

Although information security and cybersecurity are often used interchangeably, security reports are generally more information security focused with great focus to (in-) security of technology (van den Berg 2015). However, this technology needs to be operated by humans. These humans need to know how they should deal with this technology and all (in)security aspects that come with it. In order to deal with the cybersecurity aspects IT brings along, it is vital for organizations to implement cybersecurity in their governance and to create a cybersecurity policy, which also includes the implementation of CSA programs. Besides technological aspects, like active patching, using strong passwords and password managers, installing anti-virus and malware software, using a (two-way) firewall, disabling unneeded accounts and locking your computer when not in use, these CSA programs also need to focus on human aspects that cyber (in)security brings (Symantec 2016). There are several methods to understand how hackers operate, one of the well-known methods is the cyber kill chain based on the method developed by Lockheed Martin (Engel 2014).

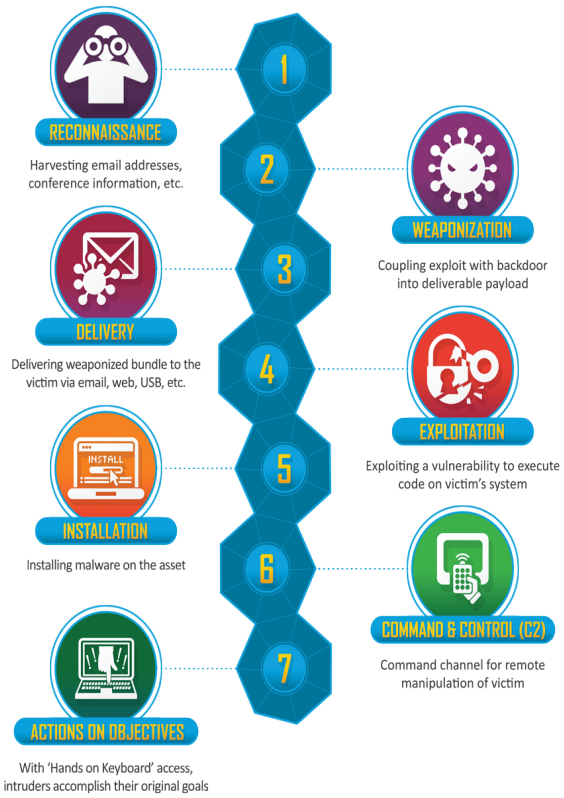


Figure 4: Cyber Kill Chain (Lockheed Martin 2011)

Reconnaissance is step 1 in the cyber kill chain, a framework to characterize cyber-attack stages, and applied to identify and prevent intrusions in the cyber landscape (SANS 2014). The cyber kill chain describes the different cyber-attack stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, action on objectives (Lockheed Martin 2011).

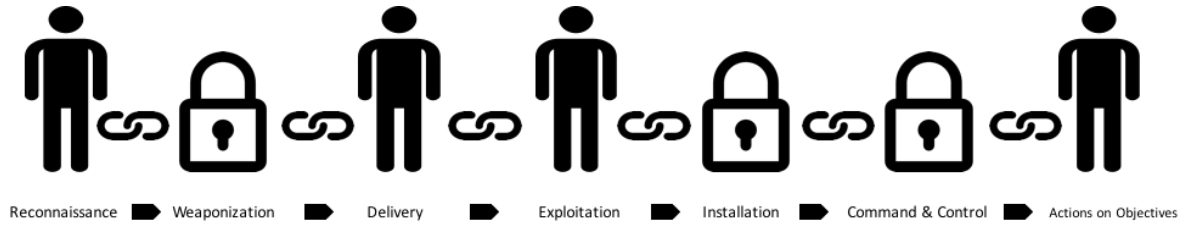


Figure 5: Human behavior in cyber kill chain

In figure 5, the Human behavior in the cyber kill chain is presented. In four places of this cyber kill chain, as shown in this figure, human behavior can be (mis)used: in the reconnaissance phase, delivery phase, exploitation phase and actions on objectives phase. These stages can be used by both the attacker and by the defender, because these stages can be used as a model of how an attacker works, and how a defender can protect its computer network. Although the cyber kill chain is a well-known model which is often used in cybersecurity, criticizers like Engel (2014) describe obvious fundamental errors. These

fundamental errors are, for example, the fact the cyber kill chain is based on perimeter defensive techniques. When an adversary knows which steps are protected, the adversary also knows which steps aren't protected.

It is clear that human behavior is a crucial link in several steps of the cyber kill chain: delivery, exploitation and actions on objectives phase, because human actions are needed in these phases. In the reconnaissance phase an attacker can use open source intelligence (OSINT) in which the attacker has to gain information about the target, which the target somehow has disclosed in open (social) media, or possibly in small talk. In the delivery phase an attacker can use a spear phishing attack in which the victim is targeted and may fall for the scam. In the exploitation phase the victim is somehow exploited because of his actions and in the actions on objectives phase gained credentials are being misused by the attacker.

In this paragraph, it has become clear although cybersecurity is an often-used term, there is no consensus on its exact meaning. However, the literature and experts in cybersecurity and CSA all agree on one thing: the human factor can be influenced throughout the realm of cybersecurity.

2.4 The psychology of scams

2.4.1 Introduction

In the previous paragraphs, it was stated in order to undermine cybersecurity, human actions can be influenced in the socio-technical layer. This influence doesn't find its origin in cyberspace, but stems from existing psychological principles that are exploited in social engineering. Therefore, further investigation to the human mind and psychological factors of social engineering is conducted, in order to generate a list of principles which is used by social engineers in their (spear)phishing campaigns.

It is not the goal of this thesis to develop new thinking in psychology. However, psychology explains why people behave as they do and explains how training can increase awareness with regard to common problems in how people distinguish and make rational judgments. This is important, because the human mind constructs its own version of reality, depending on how the information is perceived (Heuer 1999). This perception depends on previous experiences, education, cultural values, role requirements, organizational norms but most importantly the specifics of the information one receives. People tend to perceive what they expect to perceive, which is misused by scammers (Heuer 1999).

Before we further examine the psychology used in social engineering and (spear)phishing, it is first necessary to explain briefly what (spear)phishing and social engineering are, and how they relate to each other. The onion model below displays the set of social engineering techniques, phishing is a smaller subset of social engineering techniques. Spear phishing again is a small subset of phishing techniques.

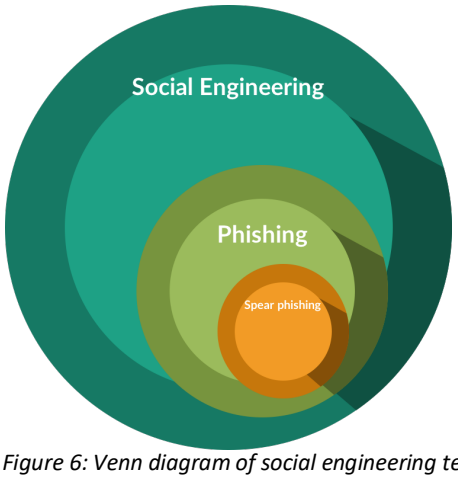


Figure 6: Venn diagram of social engineering techniques

2.4.2 Social engineering

Social engineering is a technique in which an intruder tries to access confidential information through the weakest link (humans) of a system (Mitnick & Simon 2003). Social engineering can be categorized in two groups, computer based deception and human based deception (Gulati 2003). Computer based deception is making a user think it is interacting with a computer system, for example with a pop-up in which the user has to re-authenticate due to a certain error. When the user enters the credentials as authentication, the user is deceived. Human based deception or social engineering, is to use the unintelligence and inexperience of a victim against him. An often-used method is a culprit posing as a high-ranking official calling a help desk and stating it has lost his login credentials. Because helpfulness and being liked is in human nature, the help desk employee tends to be helpful, and gets unwillingly tricked.

According to Allen (2006), social engineering consists of four phases: information gathering, relationship development, exploitation and execution.

- **Information gathering:** social engineering needs significant preparation, like gathering personal information from social media sites or performing small talk to gain trust before performing the actual social engineering attack (Harl 1997). There are many methods to gather personal information, both human based as computer based, like impersonation, riding along with an authorized user to access a restricted location (tailgating), bribing, looking over somebody's shoulders to crib credentials (shoulder surfing), eavesdropping, namedropping, looking into the trash to find confidential information (dumpster diving), reverse social engineering and phishing (Gulati 2003), (SANS 2004).

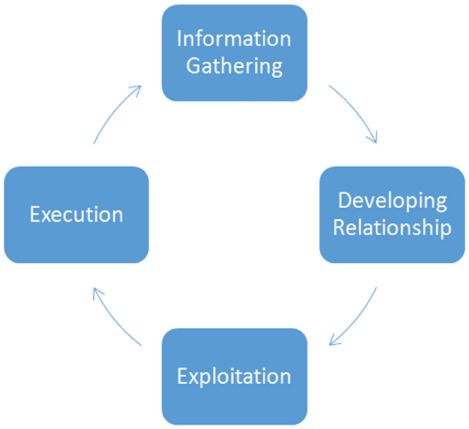


Figure 7: Social engineering attack cycle (Harl, 1997)

- **Relationship development:** The retrieved information can be adopted to build some kind of relationship (Gulati 2003) with the receiver. Standard approaches, like impersonating to be a fellow laborer, exchanging a favor, assuring the receiver the

appeal is regular, giving assurance the receiver will not be held accountable or acting just out of kindness can be used (Harl 1997). These methods can also be used in the information gathering phase, but are more effective when the attacker can already use gathered information from the previous phase.

- **Exploitation:** When some kind of trust is achieved between the attacker and the receiver, the attacker tries to somehow get access to confidential information or gets access to privileges, for example by manipulating the receivers to reveal or give their credentials, or to install some kind of exploit (Engel 2014).
- **Execution:** Now that the receiver has given access to confidential information, for example by giving its credentials or by allowing exploit software to be installed, the attacker can access the system of the receiver, breach confidentiality, integrity and availability of the information, for example by stealing, changing or deleting the information. The attacker can also proceed to the first phase of the attack cycle, because the attacker maybe now gained extra information which it can use against other, maybe more important people. The attacker can also remain in the last phase, to also have access to new information (Engel 2014).

2.4.3 (Spear) Phishing

Phishing is a specific class of email deception, through which victims are addressed by an at first sight honest legitimate sender or service, with an intent of deceiving the addressed victim of giving private information or by opening links or an attachment infected with malware which enables the phisher to perform an action the victim is unaware of (Mitnick & Simon 2003). A more focused type of phishing, where the email deception is targeted to particular persons or organizations, is known as spear phishing. Phishing is often used in cybersecurity attacks, relatively easy to design and implement, and is easy to target a bulk group. Phishing is an often used attack vector to which IT users are insufficiently aware of and therefore insufficiently resilient to (Munnichs et al. 2017).

Phishing can be combined with social engineering, which makes it even more dangerous (Teplow 2017). By making use of spear phishing, an attacker doesn't have to make use of 0-day exploits, unpatched or badly secured systems to get access. In this case, human actions lead to cybersecurity risks and vulnerabilities, both from the attackers' point of view (he will try to exploit vulnerabilities intentionally) as from the employee (receiver) point of view (he will unintentionally facilitate or permit cybersecurity incidents).

In academia, experts argue whether phishing is a form of social engineering or a way to perform social engineering (Macdougall 2012), because an interpersonal interaction is needed in social engineering. More recently, experts use a more unconstrained interpretation of social engineering, where an attacker uses the natural human bias to make persons believe something is true, regardless of the attack vector. Although the interpretations of social engineering are somehow distinct, the fundamental idea rests, because social engineering tricks a person to somehow reveal information.

2.4.4 Psychological compliance factors

What makes a receiver fall for the deception in social engineering? Regardless of the method used, the attacker makes (un)aware use of one or more psychological influence factors to influence the receiver. When these influence factors are known, these can be used in a

variety of ways to become more resilient to cyber-attacks, like addressing these influence factors in cybersecurity awareness programs, or by somehow implementing these indicators in intelligence driven cybersecurity measures.

Without knowing it, psychological principles have influence on us every day and are all around us (Weathington et al. 2011). These principles are popular tools to 'use' on us, for example in advertisements for consumer products or voting campaigns for a particular political faction. It is also a popular tool used by scientists to influence other scientist and students to use their theories (University of Minnesota 2015). These psychological influence factors are also used in scams, like phishing.

In social engineering attacks, culprits make use of (a combination of) several psychological influence factors. Mouton, Malan, Leenen and Venter (2014) published a social engineering attack model, which describes compliance principles that explain why a receiver falls for the deception of the attacker. In this model, the attacker makes use of friendship or liking, commitment or consistency, scarcity, reciprocity, social validation and authority (Mouton et al., 2014).

These compliance principles are also partly described by other well-known social engineering experts, like Cialdini (2001): reciprocity, commitment and social proof) as a weapon of influence and supplemented by Gragg (2002): strong affect, overloading, reciprocation, deceptive relationships, diffusion of responsibility and moral duty, authority, integrity and consistency. When triangulating the principles described by these three groups of experts and integrating the compliance principles of social engineering attacks, the following list of compliance principles is generated:

1. **Reciprocity:** Reciprocation is in the core of human nature. You want to be treated as other people will treat you (Mouton et al. 2014), (Cialdini 2001), (Gragg 2002). When another person gives you something (a present, information, a compliment or smile), without anything asking in return, people will feel to be in debt to that person and will have eagerness to return the favor in some form, as long as the given thing is somehow valuable for the receiver. This eagerness nullifies most alternative feelings, despite the reaction you would normally have given.
2. **Commitment, integrity and consistency:** Commitment, integrity and consistency are the psychological principles people tend to be consistent in their reactions (Mouton et al. 2014), (Cialdini 2001), (Gragg 2002). Also, when they already have started with something, they want to let other people see they are committed with the started task. People like to be seen as trustworthy, cooperative and helpful, which will result in a reaction so that the target will uphold his reputation by giving the information to the attacker. Once people start with an action, they will stand by that action, and will feel some kind of pressure to keep performing that action consistently.
3. **Social validation/proof:** People tend follow the behavior of other people in unknown, time sensitive or stressful situations, because they assume that the behavior of others is reflecting the appropriate behavior (Mouton et al. 2014), (Cialdini 2001).
4. **Friendship, liking and deceptive relationships:** People will do something for, or are influenced more easy by somebody or something they know and like, as for people or

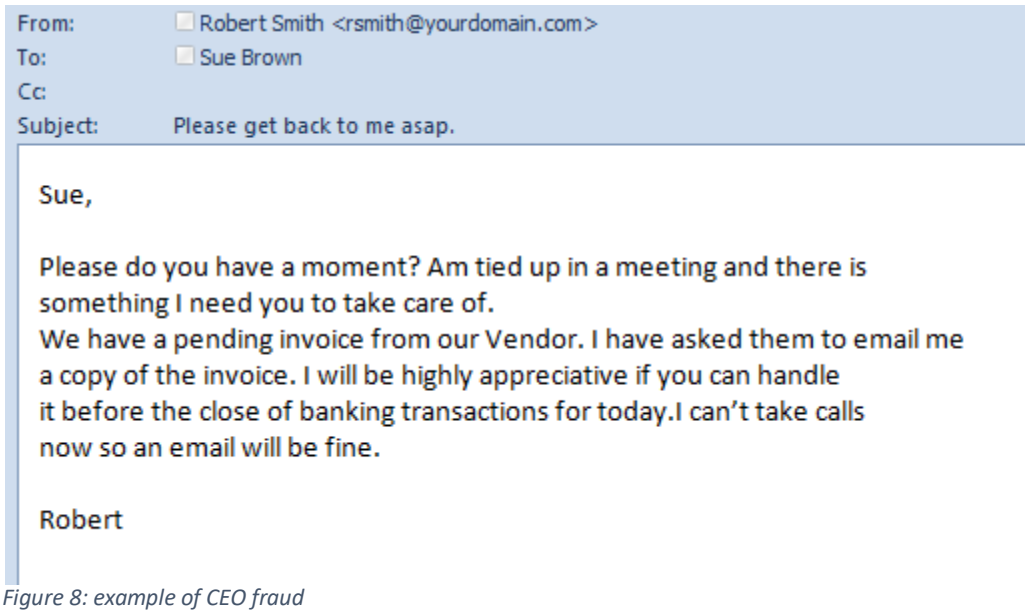
things they don't know or don't like (Mouton et al. 2014), (Gragg 2002). This can range from a beautifully designed product, to a very attractive person. This can be done for the general population, but can also be used for specific targets, as everybody has different preferences. It is therefore necessary to build on the relationship of the receiver with the attacker, which can also be done by appealing to common interests, grounds or enemies.

5. **Scarcity:** The psychological scarcity principle is used to urge a person in its decision, by letting the user believe there is a sense of urgency for his decision, because what the user wants is almost not available anymore or almost out of stock (Mouton et al. 2014). The receiver has now the feeling it has to decide immediately, values the item more than it would normally do, which ultimately leads to irrational decision making (Cialdini 2001).
6. **Authority:** People tend to comply with requests from a leading authority, as they have respect for this authority (Mouton et al. 2014), (Gragg 2002). This can be misused to get access to a location or to certain information. Authority can be divided in legal, organizational and social authority. Legal authority is established on the rules of the government, and used by government officials. Organizational authority is established on the organization hierarchy or some kind of other authority, like employee support or project groups with some kind of mandate within an organization. Social authority is established around natural leaders which 'lead' a social group.
7. **Overloading:** When people are overloaded with information in a short period of time, with illegitimate arguments hidden between legitimate arguments, people have the tendency to convert to a mentally passive social state (Burtner 1991), in which the victim doesn't evaluate the information anymore, but just absorbs and accepts the information (Gragg 2002). Because the victim has to process much information in a short period of time, this will have a negative effect on logical reasoning (Jung et al. 2014).
8. **Strong affect:** When people have strong feelings about something or someone, both positive like elation, arousal and surprise or negative like anger and fear, these feelings can be amplified by an attacker to a heightened state of emotions (Gragg 2002). These heightened states of emotions may obstruct objective or logic reasoning by the victim, and may lead to the victim agreeing with requests supported by weak arguments (Zanna 1991).
9. **Diffusion of responsibility and moral duty:** A person is made to believe that it needs to do something which it shouldn't do, for example for the greater good to prevent the boss losing his face in public, or by helping the company with a secret but very profitable takeover (Gragg 2002). The victim is assured it won't be accountable or responsible for his actions of ignoring the security policies, but is actually the company's hero and savior (Gragg 2002).

2.4.5 Analysis

There is a wide variety of scams in which psychological compliance factors are used. The Dutch NCSC was asked if there was a top-10 of most common scams in combination with a form of phishing, however due to the enormous number of scams no such list exists. Also, online research didn't reveal a clear overview. Therefore, search results from Google were used to create a general list of scams in relation to a form of phishing. It has to be noted that

variations of these scams are often used, for example: your credit card company has temporarily blocked your account and asks you to enter all your personal information. A variation is your debit bank making the same request per email, but in exactly the right typographical look and feel. In table 3, the found scams were correlated with the previously found psychological compliance factors. The scams plotted are general descriptions of scams with a wide variety of variations. For each scam, an example of that scam was used to investigate if one or more psychological compliance factors were used. For example, CEO fraud in which an attacker impersonates high ranking executives. The attacker for example asks an accounting employee to wire a large amount of money for a secret takeover or pending invoice from their vendor.


From: Robert Smith <rsmith@yourdomain.com>
To: Sue Brown
Cc:
Subject: Please get back to me asap.

Sue,

Please do you have a moment? Am tied up in a meeting and there is something I need you to take care of.
We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice. I will be highly appreciative if you can handle it before the close of banking transactions for today.I can't take calls now so an email will be fine.

Robert

Figure 8: example of CEO fraud

In the email above, Robert (CEO, authority) writes to Sue. He addresses her with her first name with a request to wire money. Sue likes to be seen as trustworthy (commitment). Robert addresses her directly asking her if she has a moment, in an apparent friendly manner (friendship, liking and deceptive relations). Robert creates a sense of urgency because it has to be wired before the close of banking transactions today (scarcity). Because Robert is the CEO and writes Sue directly, Sue is made to believe that she can do the wire and won't be held accountable (diffusion of moral responsibility and moral duty). The table below is not intended to list a complete overview of the existing scams, but is intended to find the most often used compliance factors in phishing, so they can be used in gamification of these scams for CSA-level measurement purposes.

Scam	Reciprocity	Commitment	Social Validation	Friendship, liking and deceptive relationships	Scarcity	Authority	Overloading	Strong affect	Diffusion of responsibility and moral duty
Account shut down			x		x	x			
CEO fraud		x		x	x	x			x
Bank account reactivation					x	x		x	
Unexpected present	x			x		x			
Cryptolocker	x				x	x	x		
Account upgrade			x			x			
Authority fraud						x		x	
Fake dating	x	x		x					
Microsoft helpdesk	x		x	x	x	x	x	x	

Table 3: Psychological compliance principles of widely used scams

Analyzing table 3, some psychological compliance principles stand out as being more often used than other principles. Table 3 reveals psychological compliance principles are almost always used in combination with one or more other principles and there is always some kind of time sensitiveness. This suggests compliance principles can reinforce each other and when used in combination are more effective then when used separately. It might be possible the most effective combination of psychological compliance principles is three, as the average of used principles used in table 3 is approximately three. However, this conclusion is based on minimal data, but is interesting enough to research in further studies.

The most used principle is authority, which is not surprising. People tend to listen to the authority and do whatever the authority requests. The only thing a scammer has to do is to persuade a victim it is the real authority. The three other most used principles are reciprocity, friendship and scarcity. This can be explained because in all three cases a person has an excessive desire to obtain something, a gift, attention of nice people, or an item which is not widely available, even if it doesn't deserve these things.

Commitment, social validation and strong affect are principles which can be misused by attackers because they anticipate on the urge people want others to like them, or people want to be part of something, and want other people to see them as consistent in their actions, also when they follow others and even more so when they have the same (positive and negative) feelings. However, this can also be used to increase cybersecurity. It is said humans are the weakest link in the cybersecurity chain (Mitnick & Simon 2003), however they can also be the strongest link in increasing the cybersecurity of the organization. When one announces this in one's organization, people want to be part of this popular strongest link, and are possibly more willing to pursue the cybersecurity awareness training more actively.

Overloading is another principle, in which a person cannot think rationally anymore, due to the massive amount of information which cannot possibly be processed in a short amount of time. This has a relation with diffusion of responsibility, because when a CEO asks an employee a massive request, transferring a lot of money while ignoring security policy, the employee cannot decide rationally anymore within the short amount of time given (Gragg 2002).

Mouton et al, Cialdini and Gragg all have a clear theory on psychological compliance principles, however the combination of these theories creates an even better overview. However, deceivers always try to find new methods to scam others, so there is always a

possibility to enhance and update these theories with additional psychological compliance principles.

2.5 Cybersecurity awareness training

To find information on CSA training, online research was done and expert interviews were held to arrive at a general opinion on what CSA basic training should entail. This research revealed many organizations offer cybersecurity awareness modules, however not all organizations disclose the curriculum of their training. CSA programs offered can be basic or very technical and as short as two hours and as long as one year. The focus of this thesis is on the most basic first-time CSA training being used in an organization.

In the Netherlands, there is some cooperation in cybersecurity awareness training between governmental organizations and important other organizations which do business with the government. A good example is the nationwide yearly 'Alert Online' campaign which states cybersecurity is a responsibility of everyone (NCTV 2017). During a two-week 'Alert Online' campaign the Dutch government and its partners organize several activities to enhance cyber skills and make the Netherlands more digitally secure (NCTV 2017). At first sight, it seems there is governmental coordination and stimulation in cybersecurity awareness programs within the Netherlands, however, the size of this apparent coordination and stimulation remains sporadic in nature, as appears in personal experience and in the unavailability of other coordinated programs. Due to the constant increase in cyber related incidents in the past few years (SANS 2017a), one would assume that at least every organization has its own CSA program implemented and made mandatory for all employees, but even this assumption is not the case. In fact, field research and dialogues revealed that there are even critical infrastructure organizations with no CSA program at all (Appendix B).

With CSA programs, not being compulsory at some departments and critical infrastructure organizations, this creates a security risk. Some large organizations, even the ones in the critical sector, do not have a CSA programs, and are just now planning to start this CSA for the coming years[15]. This can be explained partially by the fact cybersecurity was 'not important' and 'costly, without benefits' to be integrated in strategic processes of these organizations, because of human actions, like non-acceptance of training, risk homeostasis and the lack of proper motivation (van den Berg 2017). In order to implement cybersecurity aspects into risk management, it is important to understand who the attackers are, what these cybersecurity aspects are, and what is recommended to focus on. What is more, it is near to impossible, both from the aspects of money and time, to focus on all security aspects to protect an organization, so the focus should be well thought about (van den Berg et al. 2014).

It is important for organizations to understand what their adversaries look like in the cyber realm, and what their interests are (National Cyber Security Centre 2017). Generally, in cyberspace there are state actors, professional criminals, terrorists, hacktivists and script kiddies, sometimes complemented with internal actors and private organizations (National Cyber Security Centre 2017). All these different types of actors have different interests and resources at their disposal, ranging from script kiddies running unsophisticated hack scripts

[15] Vital Infrastructure Company 2 (2017) Interview on cybersecurity [Personal interview]

with very limited resources to just hack anything which comes at their path, to state actors using very advanced technology and having unlimited resources in order to steal government secrets or have political influence (figure 9).

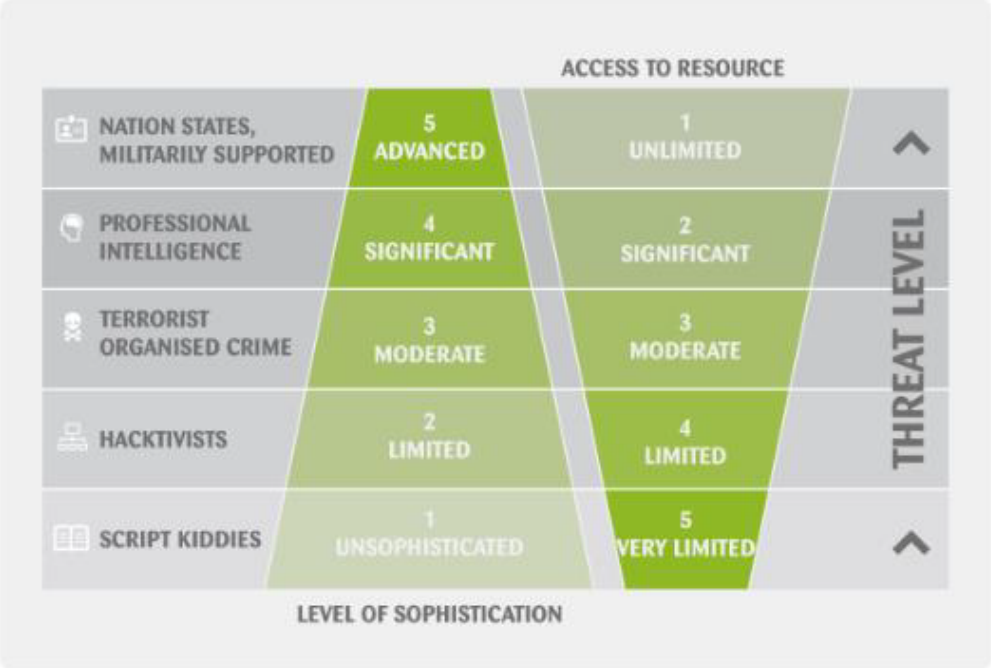


Figure 9: Current threat landscape (Fox Academy, 2017)

These cyber attackers use a variety of ways to attack persons and organizations to breach the confidentiality, availability or integrity of information of these organizations. Methods used range from very simple methods like using public available scripts to advanced and sometimes surprising methods to gain some kind of access. Some examples of new techniques are hacking into webcams and microphones of TV's while it seems the TV is off (fake-off mode) (Wikileaks n.d.), hacking into cars in order to disrupt functionality (Shipley 2017), hacking into home automation systems, for example into a smart thermostat to see if its heating and to conclude if the residents are at home (Wikileaks n.d.). Most of these examples were developed (or bought) and used by a governmental agency and not by hackers with a lower level of sophistication (Wikileaks n.d.). Although above examples are very disturbing according to cybersecurity experts like Diffie (Forbes 2014), techniques to perform these hacks are very advanced and sometimes very expensive and are not occurring on a big scale at this moment. For the future developments in the sophistication of hacks remains unknown. What is more, there are easier, cheaper and automated ways to 'hack' (WarLord 2016). A company's risk appetite should be formulated in which the security aspects that the company wants to focus on, should be assessed (NEN 2012). Although there are a lot of different opponent actors in cyberspace, all with different motives and resources available, often the easiest way to get in and most often used by all is spear phishing (F-Secure 2017; National Cyber Security Centre 2017; Brecht 2015).

Again, it is clear there also is no general opinion on what should be in the curriculum of a CSA training and which persons should attend this CSA training. Also, literature on what should and should not be in a CSA training is scarce, however using literature on how to measure CSA, these topics can be extrapolated (Kruger et al. 2006; Parsons, McCormac,

Butavicius, et al. 2014). Because there is not a lot of literature available, it is interesting if any plans are available from standardization organizations, such as NIST and ISO. NIST offers the SP800-50 (final) standard and SP800-16 standard in draft form (NIST 2003; NIST 2014), in which a lot of cybersecurity topics are described. The NIST SP800-16 standard from 2014 states that all employees of an organization should have followed basic security awareness training. The elements of basic security training are covered in the NIST SP800-50 standard which was last updated in 2003. The NIST SP800-50 standard offers 28 unstructured cybersecurity topics. The ISO 27001:2013 and 27002:2013 standards also offer topics for CSA programs, although this information is publically available it is not for free.

According to several organizations and companies which offer CSA training (University of California Santa Cruz 2017; MediaPro 2017; ESET 2017), but also according to expert interviews[16,17,18,19,20] and measurement models (Kruger et al. 2006; Parsons, McCormac, Butavicius, et al. 2014) the minimum topics which should be addressed are:

- Policies and regulations
- Physical security
- Information security
- Scams and phishing
- Password management
- Wireless and mobile risks
- Data classification and handling
- Reporting security incidents
- Social media
- Tips & tricks

Effective training address the core competences of participants, such as their decision-making principles and learning ability (Kaspersky 2017). All interviewed field experts agree all organizations should invest in their CSA training, keeping in mind not to make them too long in duration, too technical or too boring. Also, they all agree on the necessity of giving the CSA training to all employees. Cybersecurity is not only related to the cyber realm and has interfaces with the physical realm[21,22]. Also rules of conduct must be introduced to the employees before they can be addressed[23].

Some field experts emphasize the necessity of a 'couleur locale' of their CSA training[24, 25]. In other words, it is important to know your organization and the risks that apply to your organization, so these elements can be used to personalize the CSA training to your organization. Not only work-related cybersecurity aspects should be addressed in this training, but also cybersecurity related to their private atmosphere[26], as the dividing line between work and home is extremely thin.

[16] Security Company 2 (2017) Interview on cybersecurity [Personal interview]
[17] Vital Infrastructure Company 2 (2017) Interview on cybersecurity [Personal interview]
[18] Advisor DefCERT (2017) Interview on cybersecurity [Personal interview]
[19] Advisor CIO Office MoD (2017) Interview on cybersecurity [Personal interview]
[20] Vital Infrastructure Company 3. (2017) Interview on cybersecurity [Personal interview]
[21] Vital Infrastructure Company 3. (2017) Interview on cybersecurity [Personal interview]
[22] Security Company 2 (2017) Interview on cybersecurity [Personal interview]
[23] Vital Infrastructure Company 3. (2017) Interview on cybersecurity [Personal interview]
[24] Advisor CIO Office MoD (2017) Interview on cybersecurity [Personal interview]
[25] Security Company 2 (2017) Interview on cybersecurity [Personal interview]
[26] Advisor DefCERT (2017) Interview on cybersecurity [Personal interview]

Finally, although being just one of the topics which should be addressed, scams and phishing should be the main topic to be discussed as these are primarily used as first attack vector on organizations (National Cyber Security Centre 2017). Besides regular topics on cybersecurity as described above, some security companies present e-learning solutions in which phishing samples are presented. Therefore, the more specialized companies offer a real phishing attack as part of the training (SANS n.d.). However, addressing phishing or explaining scams and phishing as part of the training is a completely different expertise in relation to the psychological influence tricks which can be used. The effect of addressing scams is employees are now aware of those specific examples. However, although scams vary in design, most of the time they make use of the same psychological influence tricks. Explaining these tricks should increase the cyber resilience in general.

2.6 Conclusion

This chapter described the role of CSA in cybersecurity, by looking at cybersecurity and CSA in relation to human behavior. This was done by comparing information security with cybersecurity and by connecting it with psychological compliance factors. It was shown that existing CSA programs are still too much focused on technical aspects. Interviews with field-experts revealed focusing on just technical aspects in CSA programs is not sufficient, because of the human factor which has to control these technical aspects. Therefore, CSA training should be more connected to behavioral aspects. These behavioral aspects play an important role in social engineering and spear phishing. A more in-depth view was given on the psychological aspects of cybersecurity as these aspects can be used in CSA programs and in the conceptualization of a new methodology in chapter 5.

3 Existing models on quantifying CSA-levels

3.1 Introduction

In this chapter, a short overview is given of studies on cybersecurity awareness. Next, three approaches of quantifying cybersecurity awareness are described. The first approach is to research the existence of an awareness program in an organization and subsequently quantifying the maturity of this program. The second approach is quantifying the effect on the behavior of people of the awareness training. The third approach is using gamification to measure CSA-levels.

3.2 Quantifying specific CSA

Multiple studies are conducted on information security awareness, with the focus on one specific topic for quantifying specific CSA, instead of looking at the broader picture. All studies are based on questionnaires. Examples of these studies are:

- a study on password-related behaviors and training/awareness (Stanton et al. 2005);
- a study on security awareness in smartphone platforms (Mylonas et al. 2012);
- a study on understanding the security features within an OS and specific applications (Furnell et al. 2005);
- a study on using phishing for user security awareness (Dodge et al. 2007);
- a study on the effectiveness of information security awareness methods based on psychological theories (Khan et al. 2011).

3.3 Security awareness maturity model

To measure the maturity of cybersecurity awareness in an organization, the security awareness maturity model of SANS (SANS 2017b) can be used in order to '*easily identify where a specific security awareness program is currently at, and where a qualified leader could take it, along with an outlined path to get there* (SANS 2017b)'. The security awareness maturity model is developed by interviewing 200 security officers of different companies, and consists of five different levels:

- **Non-existent:** there is no cybersecurity awareness in the organization, employees do not know their (in)action can have effect on the safety and security of the organization, nor do they comprehend the procedures and policies of the organization;
- **Compliance Focused:** although cybersecurity awareness is implemented in the organization, this is merely done to be compliant with required frameworks. Limited random training is available, employees are not aware of their part in the safety and security of the organization;
- **Promoting Awareness & Behavior Change:** cybersecurity awareness programs of the organization are focused on key topics which have influence on those cybersecurity aspects which have the biggest impact on the operations of the organization, they increase the resilience of the organization. The goal of the cybersecurity awareness program is to have influence on the behavior or employees and to make employees understand why certain processes and policies in relation to the business context are necessary and why they, as sensors, are important for the safety and security of the organization;

- **Long-Term Sustainment & Culture Change:** cybersecurity awareness programs are implemented in the culture and life cycle processes of the organization; and
- **Robust Metrics Framework:** the cybersecurity awareness program is progressively enhanced and can be used as management information to measure the significance and gain. The cybersecurity awareness program has a visible return on investment.

The model describes the cybersecurity awareness maturity of an organization; however, the content of a cybersecurity awareness program does not mean an organization will respond 'more mature' in case of a cyber incident. SANS also states: *'Awareness is not a technical solution, it's a human solution. You need to talk with, engage, and collaborate with others – and that takes time* (SANS 2017b)*'.* The security awareness maturity model describes the existence and maturity of a cybersecurity awareness training, but not the level of cybersecurity awareness of an organization. All five steps are a combination of the implementation of a cybersecurity awareness program and human behavior. However, only the fifth level 'robust metrics framework' explains that some kind of metrics to quantify the level of cybersecurity awareness are necessary.

According to figure 10 (SANS 2017b), almost 90% of all assessed organizations are situated in the first three levels. Less than 1% try to actually quantify the level of cybersecurity awareness of the organization.

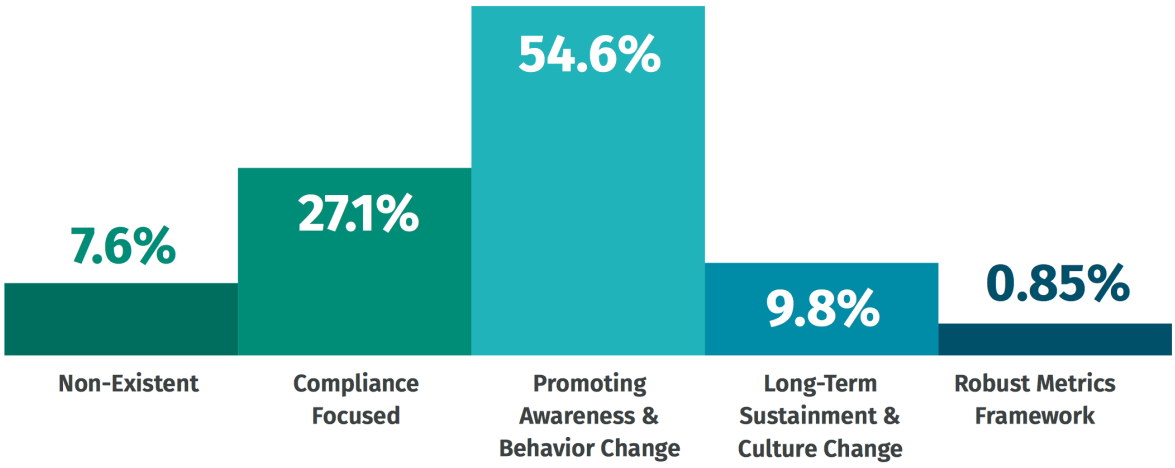


Figure 10: How mature is the average security awareness program? (SANS 2017b)

It is clear the security awareness maturity model indicates in which level of maturity an organization is, but it is unclear how the actual employees behave by using this model. Only level five presents the necessity of some kind of metrics framework, but doesn't present the actual framework itself. Although the security awareness maturity model presents insight in the maturity of cybersecurity in the organization from the implementation perspective, it doesn't reveal any useful actual behavior data (see figure 11).

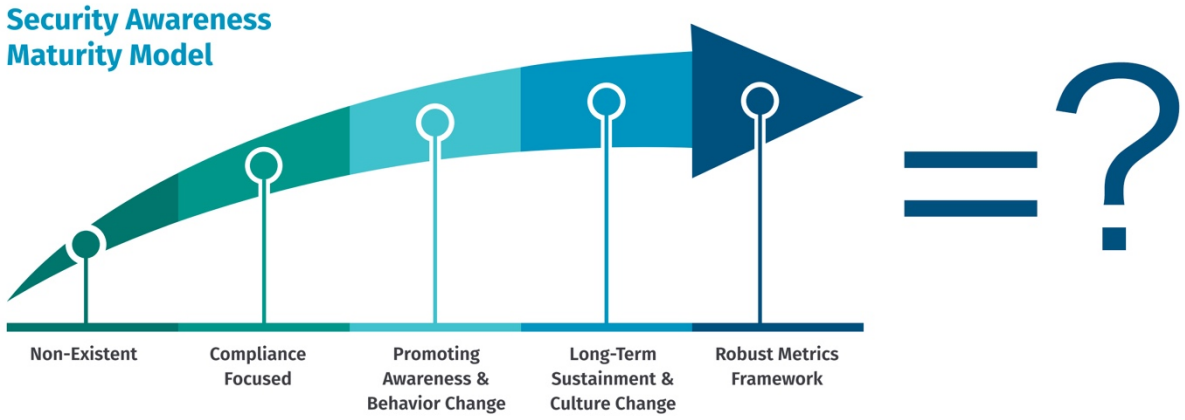


Figure 11: Cybersecurity awareness maturity model (SANS 2017b)

3.4 Cybersecurity awareness behavior measurement

In this paragraph, an overview is given of methods available for the determination of the level of cybersecurity awareness of an organization. The origin can be found in available methods of quantifying information security awareness. According to Kruger & Kearney (2006) information security awareness programs are for creating and maintaining desirable behavior that contributes positively to effective information security as a crucial part of the overall information security system. In their prototype, based on social psychology models and using surveys to measure attitude, knowledge and behavior in several focus areas, each with its own weighting criteria. It is unclear how these weighting criteria were calculated. These focus areas are:

- Adhere to policies
- Keep passwords secret
- E-mail and internet
- Mobile equipment
- Report security incidents
- Actions → consequences

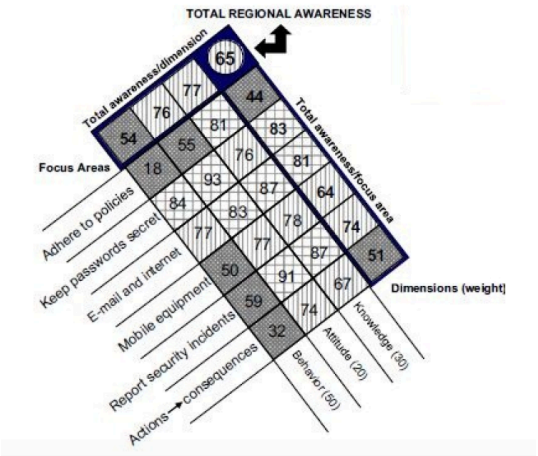


Figure 12: Example of Kruger & Kearney prototype

Figure 12 displays the seven focus areas correlated with behavior, attitude and knowledge, each with its own weight factor. Although the model gave Kruger & Kearney interesting insights, they already mentioned the model has to be validated with a physical test and could possibly be complimented with the use of automation and system data. Further developments of this model state that the privacy and confidentiality of participants should be guaranteed, by anonymizing the results and using averages (Kruger et al. 2006). Also, additional information is given on what system data to use in order to make the model more reliable. An overview of the model of Kruger and Kearney is given in figure 13 below.

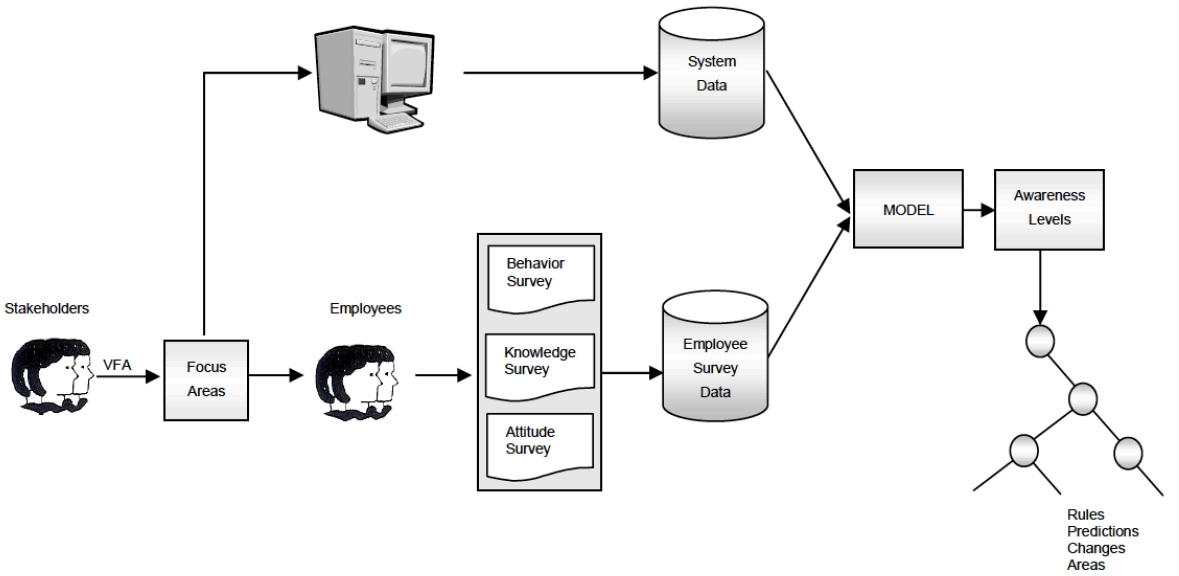


Figure 13: Framework to measure information security awareness (Kruger et al. 2006)

Figure 13 describes the K&K method, in which system data and behavioral data is combined to measure the level of awareness. Kruger & Kearney recognize the model is not finished, as they urge others to complement their studies (Kruger et al. 2006). Other researchers added a physical phishing-email test to the Kruger & Kearney model in order to validate its findings (Koroliov et al. 2009) and also used these findings to find flaws in CSA programs. Although Koroliov et al. found a correlation between the survey answers of the Kruger & Kearney model and the phishing test, their reasoning contains some inconsistencies. It is unclear if the surveys primed the employees for the phishing mail, in a manner as to which the results of the phishing mails are more a reflection of the survey, as they are on a random phishing test. However, this approach provides a good starting point for additional research.

The Human Aspect of Information Security Questionnaire (HAIS-Q, Parsons, McCormac, Pattinson, et al. 2014) uses the same concept as the Kruger & Kearney (2006) model, however, it doesn't make use of added weighting criteria for their focus areas (Parsons, McCormac, Butavicius, et al. 2014). The HAIS-Q method uses of a standardized questionnaire of 7 focus areas, each with three subcategories and 63 statements in total. Using a 5-point Likert scale, respondents give scores to these statements. The seven focus areas are:

- Internet use
- Email use
- Social media use

- Password management
- Incident reporting
- Information handling
- Mobile computing

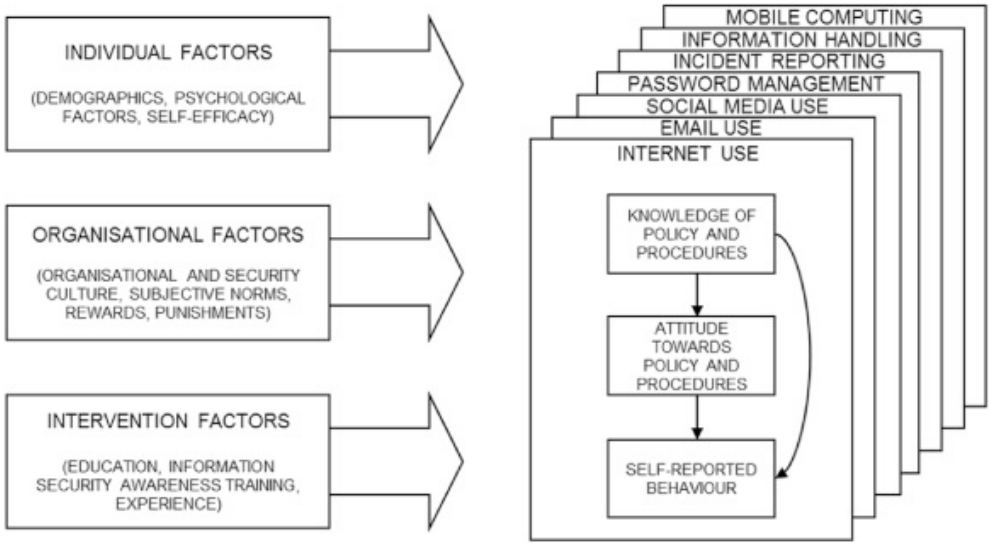


Figure 14: HAIS-Q method (Parsons, McCormac, Butavicius, et al. 2014)

Figure 14 displays the HAIS-Q method, in which several factors can be correlated with seven focus areas, each divided by knowledge, attitude and behavior. Using a test-retest reliability and consistency method the HAIS-Q method is assessed as *'a unique contribution to the information security literature and research field, as well a practical contribution to organisations* (McCormac et al. 2016)*.'* The results of the McCormac et al (2016) study are difficult to generalize because there were several difficulties with the study (inadequate sample size, respondents changing their behavior after filling in the questionnaire and possible sensitivity of the questionnaire to cultural differences) (McCormac et al. 2016; Butavicius et al. 2017). Also, the HAIS-Q method notes cybersecurity is constantly evolving, which means it is possible the model has to be revised due to new emerging threats and technological improvements (Butavicius et al. 2017).

However, HAIS-Q still is completely based on a questionnaire, from which Kruger & Kearney (2006) already stated to have possible social desirable results. At first sight, it seems the HAIS-Q method is already validated in multiple validation studies and peer-reviewed papers (Butavicius et al. 2017; Parsons, McCormac, Butavicius, et al. 2014; McCormac et al. 2016; Parsons, McCormac, Pattinson, et al. 2014), however it is remarkable that these validation studies, each time, are performed by a part of the same group of participants from the original research group, each time with another researcher as 'core-researcher'. Regardless of whether the HAIS-Q method is good, questions may be asked about the validity of this validation method.

The self-reported behavioral data that is found are completely dependent on what the respondents explain when completing the scoreboard, with the possibility of being based on subjective experience rather than facts. This data is a compromise between an easy low-impact measurement method and data with a high possibility of being the desirable answer. It is remarkable that the results of the HAIS-Q method correlate with the results of a study of

social engineering using a phishing mail as measurement (Workman 2007), because this already points to a gamification method as validation for the HAIS-Q method. Still, this data can only provide a general outline for the level of CSA without excessive complications and expenses.

3.5 Gamification as measurement method

Gamification is using elements from game design in a non-game actual contexts in order to targeted teach people skills and knowledge (Deterding 2011; Zichermann & Cunningham 2011). For example, a website and an email, integrated with a gaming mechanism. Gamification was used to validate existing CSA-level measurement methods. It is puzzling why these measurement methods use gamification as validation method, while they could also have used gamification itself as measurement method. Gamifications can be performed in laboratory experiments or field experiments (Fink et al. 2013). The advantage of laboratory experiments is a lot of elements of the experiment can be controlled in a safe environment. However, the disadvantage of laboratory experiments is the conditions are unnaturally controlled and usually are too good to be true. Field experiments however have conditions where possibly appealing real-life practice can be seen, but sometimes are impossible to observe due to complexity. Another disadvantage of field experiments is that the results can be very specific for the tested organization, as there are always specific organization conditions and unknown factors and variables that may affect the experiment, which makes the results less reproducible and generalizable. Finally, the result of gamification as measurement method is statistical data, which is an objective representation of natural behavior.

The prominent role of spear phishing in cybersecurity incidents is validated in the 91% of all cybersecurity related attacks start with some sort of social engineered phishing attack (National Cyber Security Centre 2017) and in multiple expert interviews, in which it is found that large organizations have their IT systems reasonably well in order and when these organizations are being attacked they are most affected by phishing attacks[27,28]. Phishing can be a combination of most of the focus areas of the HAIS-Q method (internet use, email use, social media use, password management, incident reporting, information handling and mobile computing), so it can be seen as a generalization of the whole method, and therefore be a useable method for quantifying the level of CSA. As mentioned before, the HAIS-Q method states their results can be validated using a lab-based phishing experiment (Butavicius et al. 2017), but doesn't describe the possibility of using the phishing experiment itself as measurement method. Kruger & Kearney (2006) on the other hand, state that simulated realistic phishing attacks can be used to find weaknesses in the response of the employees, and/or are useful to improve organizational learning (Kearney et al. 2017). However, they also do not suggest the simulated phishing attack is useful as a measurement in their K&K-method.

We conclude that phishing gamification can be both used for training as it can be used for measurement of CSA. Employees need to be trained to identify deceptive phishing (Vishwanath et al. 2011). There are several viewing points on what makes a good phishing

[27] Security Company 1 (2017) Interview on cybersecurity [Personal interview]
[28] Security Company 2 (2017) Interview on cybersecurity [Personal interview]

attack. The Vishwas triad specifies the elements of a good phishing attack (Vishwanath et al. 2016):

- a trustworthy source (such as Google, Facebook);
- a field that is usually manipulated (e.g., Google documents sender name, file name, email sender's name); and
- attack/email context which is part of the user's routine (e.g., people usually click on Google documents or click on open PDFs) or something for which they have good heuristics/thumb-rules.

According to Vishwanath, if these three things are present in the phishing mail, usually the phishing attack will be successful. In this case, the trust factor is authority. In the research of Vishwanath (2016) scarcity has little to do with the success of a phishing attack, as different attacks were performed with warnings and with rewards and neither of them work better than the other because, according to Vishwanath, people do not, generally, process that information.

However, other research contradicts this statement. In this case, an article by Sheridan (2017) reports that the most often opened phishing emails contain elements which need imminent attention, for example due to scarcity and action and misuse the desire of recognition or gratification of the recipient (Darkreading.com 2017). The most often misused words in the subject line of the email are: 'expires', 'immediately' and 'notification'. These phishing mails try to provoke a natural human response, like a sentimental response, using a concern strategy, a question which needs immediate attention, and unimaginable offers.

Although there are contradictive findings, both in proven methods like the K&K and HAIS-Q as in other research in which phishing is used as a learning method, the common theme is influencing people psychologically. Some methods use certain tricks as core item in their approach, while others don't mention them but do make use of them anyway.

3.6 Findings

3.6.1 Introduction

There are a lot of different perspectives on cybersecurity, awareness, measurement and gamification. All these perspectives have effect on cyberspace. In the past, the focus was more on information security and focused on specific areas, which is a too narrow concept in the new digital world. Also, there is no consensus on what CSA should entail and how you can measure it.

3.6.2 Cybersecurity awareness and measurement

Cyberspace not only is about technology anymore, but adds additional elements, layers: the socio-technical layer and the governance layer (van den Berg 2015). However, cyberspace cannot exist without keeping in mind the influence the physical world still has on the technical and socio-technical layer. Literature, internet research and expert interviews revealed interesting perspectives. There are several perspectives on the subjects of CSA training to increase the cyber resilience of an organization. The human factor is a very important perspective to account for (SANS 2017b). The most often mentioned subjects which have to addressed in CSA programs are correlated with the 3-layer model of van den

Berg, available measurement methods, CSA programs from security groups and expert interviews.

The kill chain model was used to illustrate the subjects have effect on human actions (Lockheed Martin 2011). Table 4 below displays the fragmented importance of these subjects. However, almost all perspectives address the following subjects, all situated in the socio-technical human action related layer: scams & phishing, password management and wireless & mobile. Scams & phishing and password management are closely related, because the latter is one of the elements scams and phishing is after. Wireless & mobile is beyond the scope of this thesis, although the wireless devices can also unlock phishing attacks. Scams & phishing will be used as a core input for a new CSA measurement framework.

Subject	3-layer model vd Berg	Literature	Internet	Interviews	Kill chain
Physical security	-	-	UCSC, Mediapro,	Security Company 2, Vital Infrastructure Company 2, KMar	Reconnaissance Delivery
Information security (CIA)	Technical layer	HAIS-Q	UCSC	Security Company 1, HDBV, Vital Infrastructure Company 1, Security Company 2, Vital Infrastructure Company 2, KMar	Full kill chain
Actions & consequences	Socio Technical layer, Governance layer	K&K	-	Security Company 2, Vital Infrastructure Company 3	-
Scams & phishing	Socio Technical layer	K&K, HAIS-Q	UCSC, Mediapro, ESET	Security Company 1, HDBV, DefCERT, Security Company 2, Vital Infrastructure Company 3,	Reconnaissance, Weaponization Delivery

				Vital Infrastructure Company 2, KMar	
Password management	Socio Technical layer, Governance layer	K&K, HAIS-Q	UCSC, Mediapro, ESET	Security Company 1, DefCERT, Security Company 2, Vital Infrastructure Company 3, KMar	Reconnaissance, Exploitation
Social media	Socio Technical layer, Governance layer	HAIS-Q	Mediapro	HDBV, DefCERT, Security Company 2, Vital Infrastructure Company 3, KMar	Reconnaissance Delivery
Wireless & mobile	Socio Technical layer	K&K, HAIS-Q	UCSC	HDBV, DefCERT, Vital Infrastructure Company 3, Vital Infrastructure Company 2, KMar	Reconnaissance Delivery Exploitation
Policies, rules and regulations	Governance layer	K&K	-	HDBV, Security Company 2, Vital Infrastructure Company 3	-
Incident Reporting	Governance layer	K&K, HAIS-Q	UCSC	HDBV, DefCERT, Vital Infrastructure Company 2, KMar	Reconnaissance

Table 4: CSA training elements

3.6.3 Gamification

Gamification can not only be used as a training method and as a validation method but also as a measurement method (Fink et al. 2013). Within all of these approaches psychologically

influencing human behavior is the common theme. The K&K-model and HAIS-Q model can be combined with gamification, not only to validate the findings in these models, but as actual measurement model, in which field experiments using phishing provide most of the measurements. In order to combine existing measurement methods with gamification, data from a case study of the gamification of a spear phishing attack will be analyzed in chapter 4. Other experiments can complement this approach but are beyond the scope of this thesis. These experiments will be shortly presented in the reflection.

3.7 Conclusion

There are a lot of different perspectives on cybersecurity, awareness, measurement and gamification. All these perspectives have effect on cyberspace. Cyberspace is not only about technology anymore, but adds additional elements, layers: the socio-technical layer and the governance layer. However, cyberspace cannot exist without keeping in mind the influence the physical world still has on it. There are several perspectives on the subjects of CSA training to increase the cyber resilience of an organization. The human factor is a very important perspective to account for.

In current interview/questionnaire measurement methods for cybersecurity awareness, in which subjects are asked about what they think, there always is the possibility respondents do not answer the question honestly, for example, because they think they should give expected or desirable answers. Although ensuring confidentiality, there still remains a high probability of answers which are somehow not a truthful reflection of the state of cyber security awareness. As no other literature is available, this information gap justifies the research being performed in this thesis. Gamification can be used as a training method and as a validation method but also as a measurement method. Psychological influence factors play an important role in this gamification approach.

4 Case studies

4.1 Introduction

This chapter describes two case studies which were done at the RNM. One is a study in which a spear phishing email is used as a measurement and training tool. The other case study is the questionnaire to measure the relation between how cyber safe a person feels in relation to how cyber safe a person acted during the spear phishing attack. Cyber safe was explained as using and feeling that (online and offline) information and communication is done safe and responsible. As the case study is a gamification of spear phishing, the results of this case study will be compared to existing CSA-level measurement methodologies described in chapter 3. Elements that can be used in the development of a new methodology for quantifying the level of CSA will be derived from the case study and used in chapter 5. The first part of this chapter describes the setup of the case study and the lessons learned from the case study. The case study is an integral part of the research. Combined with the literature study and expert-interviews it is used to reach the research goal. The second part of this chapter describes results and analysis of these results of this case study. This chapter concludes with an overview of elements and helpful lessons learned which can be used for measurement of CSA-levels.

4.2 Cyber within the Ministry of Defense (MoD)

In addition to sea, land, air and space, cyber is the fifth domain in the global threat landscape (Advisory council on international affairs 2011). In the last few years there was an increase in cyberattacks, especially focused on governmental organizations, defense industry and critical organizations (F-Secure 2017). The fifth domain is increasingly on the strategic agenda of the MoD (Hennis-Plasschaert 2014; Ministry of Defense 2015a; Ministry of Defense n.d.; Ministry of Defense 2016a; Volkskrant 2016; Ministry of Defense 2016b).

In the MoD cybersecurity strategy, the MoD has divided cyber in three realms: offensive cyber, defensive cyber and intelligence (Ducheine & Voetelink 2011). The focus of this thesis is on defensive cyber (Ministry of Defense 2012), in this case CSA and the measurement of CSA-levels. The case study is done within the Royal Netherlands Marechaussee (RNM), internationally better known as the military police, one of the 4 services of the armed forces of the MoD (Army, Navy, Airforce, Marechaussee). The RNM works closely together with the Ministries of Internal Affairs, Foreign Affairs, Justice and Security and Defense. Besides working closely together with other Ministries, the RNM also works with other large organizations, both in the field of security as well as in the critical sector. In 2016, the RNM made CSA training mandatory for all their employees as the first of the 4 services that make up the MoD. Every employee of the RNM needs to have done basic CSA training before December 31, 2017.

Because of the forerunner cybersecurity position of the RNM, and the close participation with other Ministries and cybersecurity organizations, the RNM is a useful organization to perform the case study. The RNM is an organization with unique characteristics in security in general, due to their specialism in military training and law enforcement and because their employees are both military and civilian (Baarda & Verweij 2006; Staf Commandant KMar 2015). The RNM has around 6200 employees (Ministry of Defense 2015b), consists of a Staff group, a National Center for Training and expertise and 25 brigades (Defensie.nl 2017). The Staff group supports the Commander of the RNM with the execution of its tasks. Operational

Marechaussee employees are trained at the National Center for Training and Expertise. All operational tasks are executed by the brigades, and are part of the National Tactical Command.

4.3 Case study 1: Phishing as training tool

4.3.1 Introduction

According to the yearly publication of Dutch National Cyber Security Center of the current cyber security situation of the country (Cyber Security Beeld Nederland -CSBN- 2017) cyber espionage and cyber criminality keep on being the biggest threats for governmental organizations and businesses (National Cyber Security Centre 2017). The NCSC (2017) report states that State and criminal actors are developing their attack skills faster than before. For example, attackers are using active reconnaissance effectively to scale their operations and to increase their attack infrastructure, so they can automate their phishing campaigns, while still making them less easy to distinguish from an original email (F-Secure 2017). As stated before, according to the NCSC, 91% of all hacks start with some kind of phishing (National Cyber Security Centre 2017). In these circumstances, the measurement of the results of a directed phishing campaign is a very good indication on the level of cybersecurity awareness of an organization.

4.3.2 Design of the spear phishing case study

The RNM, together with Kennis Innovatie Experimenten en Simulatie-centrum (KiXS) developed an experiment intended to find out, whether the current state of cybersecurity awareness could be measured and train employees at the same time. This was done through a social engineered spear phishing experiment, with the aim to find out how employees truly behave when being phished (Kruger et al. 2006) .

Because the spear phishing was intended as a proof of concept to be used as a training exercise it was not specifically designed for the research of this thesis. As such there was no rigid experimental design in which subjects from the RNM were randomly chosen (random sampling) and randomly assigned to different experimental sample groups to be compared to each other or compared to a control group that did not get the experimental treatment. With the current experimental design, it is not even clear what the experimental treatment is, as for the training case, the experimental treatment is the phishing mail, but for the measurement of CSA, the experimental treatment is the cyber security awareness training itself. For either set-up, apart from having no random sampling and no random assignment to sample groups, there also were no control groups no treatment at all (either no training or phishing mail).

Case study 2, described in paragraph 4.4 was specifically done to alleviate some of these problems. The experiment was performed three times, to three different sample groups, with a total number of experimental subjects of n=560, from a population size of 6200 employees. All employees work within the Netherlands for the RNM.

The subjects were divided in three sample groups, the treatment here being the cyber security awareness training. General population information is given in table 5. However, the treatment was not divided over the sample groups, but within each sample group there were subjects that had the training and there were subjects that did not had the training.

The was no control group (with no training at all). The total sample consisted of 560 employees.

Sample group	Group A	Group B	Group C
Group size (n)	280	99	181
Man	187	73	138
Women	93	26	43
Civilian	138	31	28
Military	142	68	153
Age Mean	46,79	44,83	42,12
Age SD	10,06	8,74	9,29
Training	72	39	18
No Training	208	60	163

Table 5: population information

Group A, the Strategic Staff group had *n=280 subjects*, and received their cybersecurity awareness training > 1 year before the experiment.
Group B, the Staff groups of the National Tactical Command had *n=99 subjects* and received their cybersecurity awareness training <1 week before the experiment.
Group C the Staff group of the National center for Training and expertise had *n=181 subjects* and received their cybersecurity awareness training < 1 year before the experiment.

Employees were not informed they were part of an experiment for the duration of the experiment. After the experiment, the employees received feedback of the experiment, including a general description, and feedback about how they had handled and should have handled during the experiment.

4.3.3 Method used in case study 1

Although there were some privacy and security problems with this experiment it was approved by the Defense Security Authority, the Security Commander of the RNM and the privacy officer of the RNM. Also, to keep control over the experiment at all times effect, the execution of the experiment was monitored by the internal CERT organization of the MoD (DefCERT), and other key partners within the MoD. To ensure that the subjects involved in the experiment did not know beforehand they would be exposed to a simulated phishing mail, the details of the of the phishing experiment were only shared with a select group of people. To comply with security and privacy requirements subject-identifiable data was coded and dispersed over different data files whereby not all researchers had access to all of the data. Only one person had access to all the data.

After getting approval of the Security Commander of the RNM, the first sample group (group A) was selected and their contact information was provided by the human resource department. The sample group A (Strategic Staff of the RNM) was selected for the first sample group of the experiment, because of two reasons; to serve as an example for the rest of the RNM and because this group would not have an effect on operations in progress.

After the first experiment (group A) was finished, interesting conclusions were made. The general impression of the employees was they learned more from the phishing example in contrast with existing CSA training. Moreover, the experiment revealed interesting data concerning the in percentage negative results of CSA trained employees in relation to untrained employees which in percentage scored better. Discussions revealed employees could indicate malicious emails, but because they assumed the security at work was proper, they acted like the email was safe. Should they have gotten the same email at home, they would not have opened it.

It was decided to conduct a second and third experiment, in order to target a similar group size. The second and third group (group B and group C), were chosen, due to their 'non-operational' nature, so the experiment would not interfere with ongoing operations. In this second and third experiment, a few minor changes were implemented due to lessons learned from the first group. The most important change was informing additional important stakeholders within the MoD, like Security Commanders of other operational commands, to prevent a possible mixture with the contained experiment in active out of scope operations.

Because the experiment was a proof of concept, not all processes could be automated. The Security Commander approved the data could be accessed and used by a select group of people, with the restriction that the names and the email addresses needed to be anonymized in the final report. Only statistical data could be used. To be able to target the group, KIXS also got access to the email addresses. These email addresses were used to send the spear phishing experiment to the sample group.

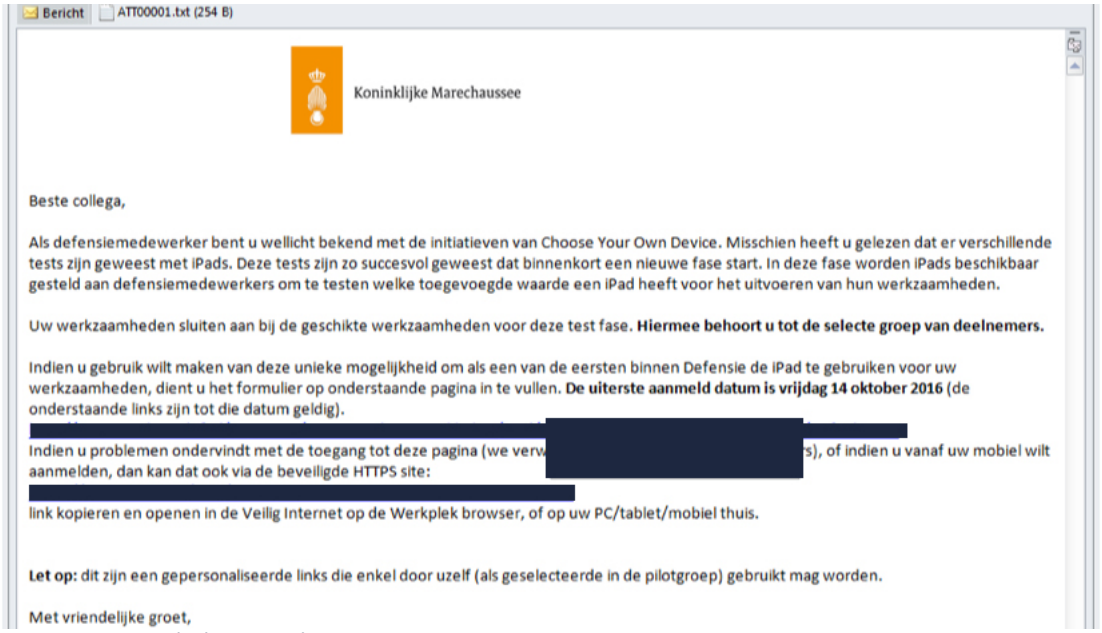
The experiment with the first sample group (group A) not only yielded interesting data on security awareness, but also provided important lessons on how to improve upon the execution of the phishing experiment, which improvements had to be implemented before other sample groups could be targeted. As mentioned earlier, just a select group of people were informed about the phishing experiment. However, although it was thought all the necessary people were informed, it became clear some key officials were forgotten, which could have led to unwanted mitigation actions interfering with the experiment. One of the unforeseen actions of targeted employees was forwarding the email with good intentions to other colleagues outside the sample group, which led to 'infection' and no control outside the contained sample group. It also became clear employees didn't know where and how they could file a report on receiving a phishing mail.

Subsequently, after the experiment with sample group A some modifications were made to the setup of the experiment. Additional key stakeholders were informed and the target email and website were slightly altered, because of the possibility of the leakage of information about the experiment. However, the changes made were minimal so that the following phishing experiments were to be as similar to the initial experiment as possible. The subjects in sample group A were promised an iPad. The subjects in sample group B and C were promised the updated version of the iPhone. In essence, the setup of the email and website were exactly the same for all three sample groups, only the promised iPad was changed to the new iPhone with fingerprint recognition. The experiment with sample group A was done in October 2016. Sample group B and sample group C were send the phishing

mail in February 2017. For each sample group, the experiment had a duration of four working days.

4.3.4 Phishing set-up

In the phishing experiment, three most common used psychological influence factors, authority, scarcity and reciprocity were used to trick employees into believing the phishing mail (Mouton et al. 2014; Cialdini 2001; Gragg 2002). Although not explicitly chosen for this case study, the experiment also adheres to the SCAM model of phishing susceptibility (Vishwanath et al. 2016) in which the Vishwas triad is essential: a trustworthy source, a field that is usually manipulated and attack/email context that is part of the user's routine. Experiment 1.1 was conducted at the end of 2016. Subjects were sent an email which was spoofed and 'trusted' (Vishwanath et al. 2016) (no-reply@mindef.nl; %Projectteam voor iPads Defensie). This email contained three often used social engineering principles (Mouton et al. 2014; Cialdini 2001; Gragg 2002): authority (projectteam voor iPads Defensie), scarcity (only a select number of iPads/iPhones available) and also using a time sensitive period of registration possibility.


Bericht ATT00001.txt (254 B)

Koninklijke Marechaussee

Beste collega,

Als defensiemedewerker bent u wellicht bekend met de initiatieven van Choose Your Own Device. Misschien heeft u gelezen dat er verschillende tests zijn geweest met iPads. Deze tests zijn zo succesvol geweest dat binnenkort een nieuwe fase start. In deze fase worden iPads beschikbaar gesteld aan defensiemedewerkers om te testen welke toegevoegde waarde een iPad heeft voor het uitvoeren van hun werkzaamheden.

Uw werkzaamheden sluiten aan bij de geschikte werkzaamheden voor deze test fase. **Hiermee behoort u tot de selecte groep van deelnemers.**

Indien u gebruik wilt maken van deze unieke mogelijkheid om als een van de eersten binnen Defensie de iPad te gebruiken voor uw werkzaamheden, dient u het formulier op onderstaande pagina in te vullen. **De uiterste aanmeld datum is vrijdag 14 oktober 2016** (de onderstaande links zijn tot die datum geldig).

[redacted]

Indien u problemen ondervindt met de toegang tot deze pagina (we verw[redacted]s), of indien u vanaf uw mobiel wilt aanmelden, dan kan dat ook via de beveiligde HTTPS site:

[redacted]

link kopieren en openen in de Veilig Internet op de Werkplek browser, of op uw PC/tablet/mobiel thuis.

Let op: dit zijn een gepersonaliseerde links die enkel door uzelf (als geselecteerde in de pilotgroep) gebruikt mag worden.

Met vriendelijke groet,

Figure 15: Spear phishing email

The spear phishing email contained two links, one to a (non-existing) internal webpage to gain trust, the other, should the internal link not work due to overload of people trying to access the internal page, to a seemingly legitimate page on internet, but with a tampered hyperlink (mindefS.nl) and to a fake website. The second link contained a user specific hash, derived from the email address, in order to be used for monitoring purposes. Both links were monitored and logged by DefCERT. Also, for measurement purposes, the link to the internet-web page was unique for each subject, and generated through a hash of the email address.

The internet web page used the branding of the RNM and contained some obvious flaws like typos, wrong branding and strange requests. These flaws to the internet page were intentionally added to make the web look more like a real phishing web page, thus making

the experiment more realistic. If a subject wanted to apply for the free iPad/iPhone, the subject had to enter its company credentials (login/password). The website checked if the credentials entered adhered to the security policy of the MoD (correct number of login numbers/digits and the correct minimum characters of the password). The connection to the internet web page to which the phishing email linked was encrypted with the use of a https-certificate.

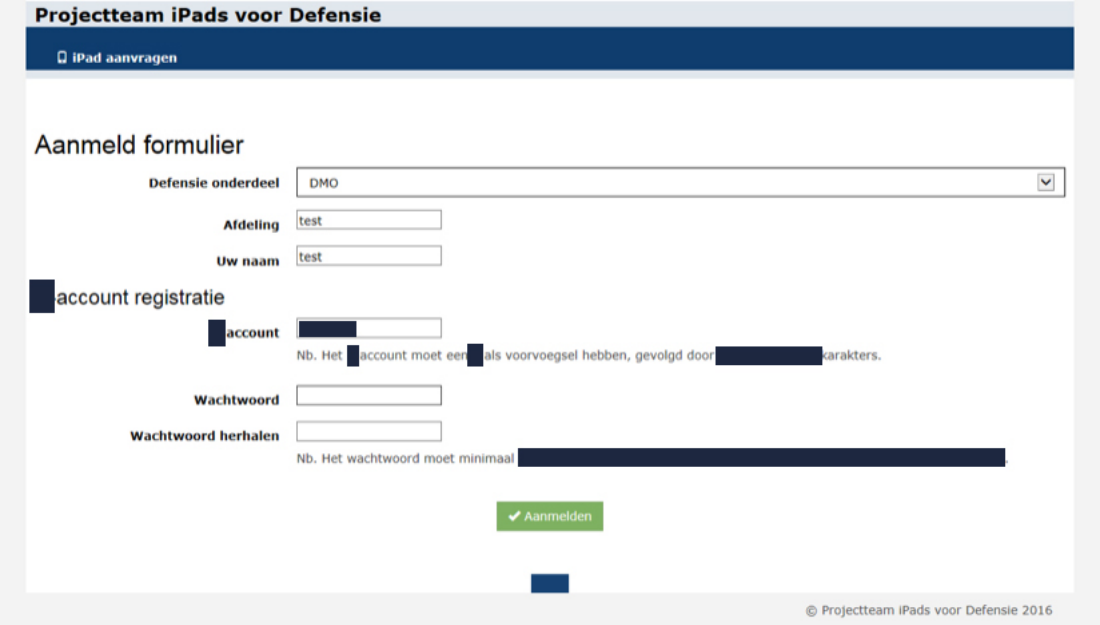


Figure 16: Fake website

There were 8 different reactions possible in case study 1:

1. No reaction at all;
2. Opening of the internal webpage, but nothing more;
3. No opening of any links, but with filing of a report;
4. Opening of the internal link, but with filing of a report;
5. Opening of the internal and external link, not leaving any information, and with filing of a report;
6. Opening of the internal and external link, inputting information on the fake website, and with filing of a report;
7. Opening of the internal and external link, inputting information on the fake website, and not filing of a report;
8. Opening of the internal and external link, not leaving any information and not filing a report.

4.3.5 Results of the phishing experiments

In figure 17 below, the timeline of experiment with sample group A is shown. During four working days, the campaign was active.

- first employee reported the spear phishing after 41 minutes;
- after 1 hour, 20 employees had clicked on the link in the email and entered their credentials on the internet web-page.

- within 24 hours, 70 employees had clicked on the link in the email and entered their credentials on the internet web-page;
- after 24 hours, a department head sent a warning email to a part of the treatment group, after which there is a significant drop in the growth of subjects responding by clicking and entering their credentials;
- in total 85 subjects (of 260) clicked on the link to the internet web page and entered their company credentials there.

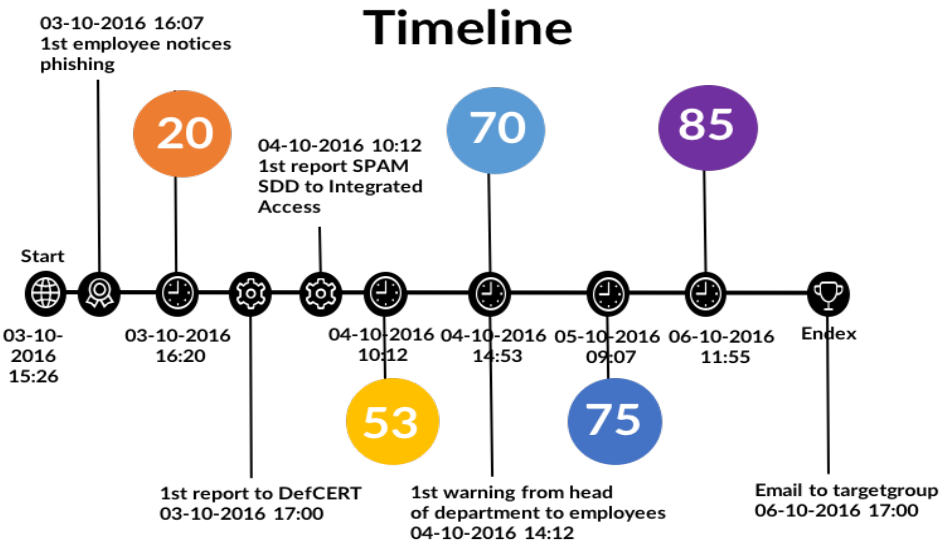


Figure 17: Timeline of phishing experiment sample group A

As the RNM was only interested in general results, the table 6 below displays the results of group A, B and C.

	Size (n)	Received training	Of which not in compliance with security policy	Did not receive training	Of which not in compliance with security policy
Group A	280	25,7% (72)	43,1%	74,3% (208)	28,8%
Group B	99	39,4% (39)	33,3%	60,6% (60)	23,3%
Group C	181	9,9% (18)	33,3%	90,1% (163)	14,1%

Table 6:training vs not in compliance with security policy

In this case, we made a comparison between acting or not acting in compliance with the security policy. The total target group was 560 subjects, 431 did not receive a cybersecurity awareness training, 129 did receive a cyber-security awareness training. From all subjects who did not receive the cybersecurity awareness training, 22,5% did not respond in accordance with the security policy. From all subjects who did receive the cybersecurity awareness training, 38,8% did not respond in accordance with the cybersecurity awareness

training. Comparatively, employees who attended a cybersecurity training scored worse in the phishing experiment in comparison with employees who did not attend a cybersecurity training. Although this result is remarkable, it is not unique. Multiple studies revealed the same findings, but were not able to explain these findings[29] (Mourik 2017).

Overall group A had the worst score on acting in compliance with the security policy, for both the group who received their training and the group who didn't receive their training. Because group A also is the group which received their cybersecurity training more than one year ago, this might indicate a drain of knowledge with the passage of time. In this analysis, group B and C performed equally, comparing the results of the employees which had followed the training, but did not act in accordance with the company policy. To find out if other factors played a role, the data was clustered; age in four groups, commission in three groups and three groups in both military as civilians. Given this database D, we found all the data points $X \in D$ having the top-n largest (worst) and top-n lowest (best) anomaly scores for f(x). With the data at hand, a profile was created in regard with the normal behavior, in our case the summary of the total population and their overall behavior. Next, this profile was used to be able to discover deviations which were considerably different from the normal profile.

Action	**Points**
Click on internal link	10
Click on external link	40
Leaving information on rogue website	60
Not filing a report	20

Table 7: Score system in experiment

In table 7 a scoring mechanism is described through which a score can be calculated for each of the different decisions. The points in the score mechanism is arbitrarily chosen, and results in a logical score. A higher score means having made more wrong decisions.

	Population research (N=560)	**Worst score / in all occasions 'wrong decision'(N=119)**	**Best score / in all occasions 'correct decision' (N=10)**
Gender	71% man (398) 29% women (162)	71% man (85) 29% women (34)	70% man (7) 30% women (3)
Age	14% until 34 years (80) 31% 34/44 years (171) 31% 44/54 years (172) 24% 54 years and above (137)	12% until 34 years (14) 32% 34/44 years (38) 32% 44/54 years (38) 24% 54 years and above (29)	10% until 34 years (1) 40% 34/44 years (4) 50% 44/54 years (5) 0% 54 years and above (0)
Commission	63% Militairy (352) 33% Civilians (186) 4% External hiring (22)	61% Militairy (72) 39% Civilians (47) 0% External hiring (0)	70% Militairy (7) 30% Civilians (3) 0% External hiring (0)
Rank category	1% Homages (5)	3% Homages (2)	0% Homages (0)

[29] Vishwanath, A. (2017) Email correspondence on cybersecurity [Personal interview]

	37% Non-commissioned officers (130) 39% Officers (217)	32% Non-commissioned officers (23) 65% Officers (47)	29% Non-commissioned officers (2) 71% Officers (5)
Civilian scale	6% t/m 5 (11) 17% 6 t/m 8 (31) 77% 9 and higher (144)	4% t/m 5 (2) 21% 6 t/m 8 (10) 74% 9 and higher (35)	0% t/m 5 (0) 0% 6 t/m 8 (0) 100% 9 and higher (3)
Group	50% Group A (280) 18% Group B (99) 32% Group C (181)	63% Group A (75) 17% Group B (20) 20% Group C (24)	50% Group A (5) 30% Group B (3) 20% Group C (2)
Training followed	77% No (431) 23% Yes (129)	66% No (78) 34% Yes (41)	40% No (4) 60% Yes (6)

Table 8: Control group vs worst score vs best score

Table 8 compares three selections: results from the total group (N=560), results from all the persons with the worst score / in all occasions 'wrong decision'(N=119) and results from all the persons with the best score / in all occasions 'correct decision' (N=10). In these three selections, a comparison is made with different population information: gender, age, commission, rank category, civilian scale, group and training followed. Based on the table 8, it may be concluded there is no difference in making the correct or the incorrect decision; both women as men in all groups are as much represented. In the category age, there is little difference in making the wrong decision, when comparing the group average between the three target groups.

At first sight, little information can be found when comparing the results with the population, however age seems an important factor. For instance, no 'good decisions' are made above the age of 54. The highest good decision rate can be found in the age range of 34-54. When looking at the group 'worst score' and comparing it to the group mean, in percentages there are more civilians. When looking at the group 'best score' and comparing this to the group mean, in percentages more military personnel can be found. It is notable, although the numbers are minimal, military officers in percentages are more represented in both groups (best and worst score), compared to the group mean.

The population civilian scale 6-8 makes more often a 'wrong' decisions compared to the total population; although these statistics were derived from a small subset of the dataset. Compared to the general group mean, group A more often made more 'wrong decisions', in contrast to group B, which made more 'correct decisions'. This might be related to the moment these groups were trained; personnel which were trained in group A had their training more than one year ago, while personnel which were trained in group B had their training in the week previous to the week they were part of the experiment. It is remarkable, that employees which have followed the cybersecurity awareness training are more present in the group 'worst score' and 'best score'.

	Click on internal link	Click on external link	Input on rogue website	Filed a report
No training followed	36% (153)	23% (97)	19% (83)	4% (17)

(N=431)				
Training followed (N=129)	55% (71)	39% (50)	33% (42)	7% (9)

Table 9: training vs results

We already found that employees score worse when they had followed the training in comparison with not having had the training. However, the table above shows indications based on percentages of employees who had training more often filed a report in comparison with employees who did not had the training.

The questionnaire of case study 2 revealed employees act less secure at work in comparison with how they act at home. One of the main reasons is they feel more secure at work, because they are under the assumption company IT security will protect them against all cyber threats. The overall cybersecure feeling at work is given a score of 7.91, while the overall cybersecure feeling at home is given a score of 6.70. This result is in line with a recent publication of the Dutch NCSC (Alert Online 2017). This is an important result, which has to be used in further development of training (knowledge), in order to change the behavior and attitude of the employees. This result is beyond the scope of this thesis, but is interesting to investigate in further studies.

4.4 Case study 2: Spear phishing as CSA measurement

4.4.1 Introduction

Case study 2 was done specifically for this thesis, to investigate if the gamification of spear phishing can result in useful data for CSA-level measurement. As described in 4.3.3, discussions after the experiment with group A revealed employees sometimes opened and acted on the phishing email, even though they were able to indicate it was malicious, because they were feeling cyber safe within the network of the MoD. At home, they would not have opened the email. This revealed information could be used to research if there was a difference in the cyber safe feeling at work in relation to at home, but more interestingly, could also been used as indicator if a safe feeling could be compared with safe acting.

4.4.2 Design of case study 2

The new-found information was used to create the second case study. The objective of case study 2, was twofold. First, additional information was necessary, to get an understanding how cyber safe employees feel when they are asked for information in a questionnaire, secondly this was put in contrast with how (un)secure employees act when they are not aware their actions are monitored (as in case study 1).

Case study 2 is done to find out if the results of a spear phishing exercise give a more realistic measurement of the level of awareness of an organization than measurements with questionnaires. The same sample groups as in case study 1 were used. Sample group A received their cybersecurity awareness training > 1 year before the experiment. Sample group B received their training <1 week before the experiment and sample group C received their training < 1 year before the experiment.

However, in case study 2 all three sample groups are taken together. The comparison made is between the answers on the questionnaire and the response on the phishing mail in case study 1, allowing to investigate the possible difference between self-reporting and actual behavior. With this information an assessment of the validity of current, questionnaire based, measurement methods are made. The data found can also be used to validate the proposal for the design of a new methodology as described in chapter 5.

4.4.3 Method of case study 2

In order to acquire the additional information needed in case study 2, an email based questionnaire was used to have the subjects self-report on their (supposed) security behavior. This questionnaire was designed to have a completion time of less than five minutes. In the accompanying email this was explicitly mentioned, in order to get a higher response rate. Also, a reminder email was sent after one week, in order to get an even higher response rate.

The questionnaire had 3 questions in the form of 2 Likert scale questions. This was done by asking the employees to give a score (1 low – 10 high) how cyber safe they feel at home and how cyber safe they feel at work in order to assess if the results from a questionnaire are comparable with the results from the phishing experiment. The third question was an open question, in which the subjects were asked why they acted the way they acted in the phishing experiment. These results were not used in this thesis, but are transferred to the RNM for evaluation purposes.

The resulting data of case study 2 was gathered in a separate file, using the same structure as the data file of case study 1. For security and privacy reasons, the subject names were hashed using the same algorithm as used in case study 1 after which the data was merged with the anonymized dataset from case study 1.

4.4.4 Results of case study 2

As mentioned earlier, a survey was send to all employees from group A, B and C, in order to research how cyber safe they feel at work and at home. The first response rate was 26% however after a follow-up email the total response to this email survey was 39,5%. The number of reactions on the questionnaire was 221 out of 560. The general results of this questionnaire are displayed in table 10.

Group	*Employees responded*	*Safe feeling mean work*	*Safe feeling mean home*
A	118	7,97	6,57
B	44	7,98	6,83
C	59	7,77	6,8

Table 10: cyber safe feeling at work and at home

Although some measures were taken to protect the privacy of the respondents and the security of the organization case study 2 still yielded some surprise lessons. For instance, not

all employees were enthusiastic about the earlier phishing study and/or the questionnaire, which resulted in some aggressive responses. Measuring how many reports were filed was one of the research goals of case study 1. However, because some of the employees had the feeling they were personally attacked, they did file a report on the phishing mail after receiving the questionnaire, but these were at this stage, not monitored anymore. Because the case studies were not reported to all stakeholders within the MoD, these filing of reports resulted in internal investigations.

4.5 Data analysis of case study 1 and case study 2

4.5.1 Introduction

Case study 1 (the phishing experiment) was conducted within the RNM (N=6200). As mentioned before, the goal of the experiment was to serve as a proof of concept for training purposes. Therefore, there was no rigid scientific experimental design made for the experiment. However, some simple statistical analysis of the results could still be made. Analysis on case study 2, was done by taking more information on the subjects into account in the analysis and by including the analysis of the results of the additional questionnaire. In the further analysis of the results, no distinction is made between case study 1 and case study 2, because the complete dataset is used. A partial display of the dataset is added in appendix B.

4.5.2 Remarks on a scientific design and correct sampling scheme

As the phishing experiment executed at the RNM was not intended for scientific research, it was not instigated as scientific research. However, when you want to use this gamification as CSA-level measurement, it has to be reproducible and validated, which means it has to meet to basic principles for statistical research.

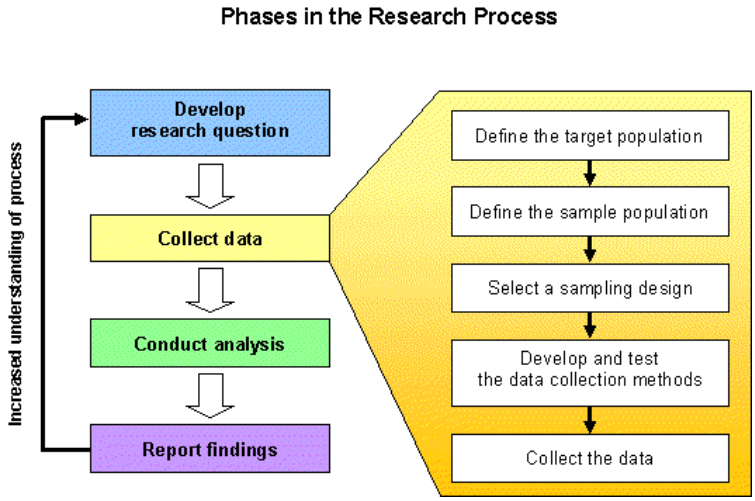


Figure 18: Phases in the research process (University of Victoria n.d.)

In the case of the RNM, we self-selected the sample groups, to research if a phishing experiment could be used as measurement and training mechanism for CSA. The collection of data in the experiment of the RNM was performed in the following manner:

- The RNM was selected as target population (N=6200);
- Three groups were sampled out as subset of the total population, as it was impossible to make use of the total population (n=560);

- Because the experiment was intended as proof of concept, without a scientific reasoning, using backwards reasoning the sample design was non-probability sampling, this convenient targeting had four important reasons:
    - The position of the thesis writer in the organization, as part of the advisory group of the security authority of the RNM;
    - The modus operandi of the MoD is learning by example. The three targeted Staff groups were used as a cross section of the RNM, in which the Staff has to be the example of its employees;
    - Because only the Staff groups were targeted, the operational executive groups were unaffected. Therefore, running operations were not affected; and
    - The tradeoff between internal and external validity.
- The phishing experiment was performed three times, after the first time, the experiment was slightly tweaked; and
- As mentioned in 4.3.5, figure 17, only little data was collected.

The only analysis performed is displayed in figure 17 in 4.3.5, which was reported to several boards within the MoD. Next, it was decided the data collected in this experiment could be used in this thesis. As mentioned before, the approach of this case study was not scientific. Therefore, basic scientific steps were not taken, which is important to have a validated method. To get an increased understanding of how the process should have been performed, these steps are described using data from the case study. As the sample it the RNM (N=6200), the needed sample size has to be calculated (Surveymonkey.com n.d.):

Unlimited population: $$n = \frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2}$$

Finite population: $$n' = \frac{n}{1+\frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2 N}}$$

Figure 19: formula to calculate minimum sample size

Total population of RNM *N=6200*, the number of employees phished in relation the whole population: *p=560/6200*, the desired confidence level: 95% (*z-score:1.96*), basic margin of error = *5% (ε).* This results in: **sample size needed: n=362.** Should the case study have been performed in the correct manner, using the correct probability sampling methods, the used sample size of 560 persons would have been sufficient. What is more, it could have been 198 employees less. This sample reflects the benefits of conducting science in the proven ways, as in this case, less employees had to be targeted.

4.5.3 Analysis of the questionnaire results

4.5.3.1 Margin of error

Additionally, in the second case study a survey was send to the entire sample population of the first case study (*N=560*). The first response rate was 26% however after a follow-up email the total response to this email survey was 39,5%, *N=221*, (p=221/560). Using basic statistics, the margin of error for a proportion can be calculated with the following formula (Ncalculators.com n.d.):

$$ME = z\sqrt{\left(\frac{p(1-p)}{n}\right)}$$

Figure 20: formula to calculate margin of error (ME)

Using a 95% confidence interval (z-score:1.96), this results in a margin of error of 4.04%. The calculated margin of error tells how effective the response of the questionnaire is. Therefore, it is stated the smaller the margin of error is, the more confidence you can have in your results, in this case our questionnaire with the **confidence interval of 95%** and a **margin of error of 4%** means that the results of the questionnaire are a reflection of what the population thinks between 91% and 99%.

4.5.4 Questionnaire data vs measurement data

Subjects were asked how cyber safe they feel at work and at home (paragraph 4.4.4, table 10). As the phishing experiment was also conducted at work, the results of case study 1 can now be compared with the scores on the question in the questionnaire on how safe the subjects feel at work. We will analyze the correlation between (non)safe acting correlates and (non)safe feeling. Data from the phishing experiment is only used when the same subject also gave a response on the questionnaire in case study 2. Although the HAIS-Q methodology measures 63 statements with seven focus areas and the comparison of this paragraph only compares two overall results, it still indicates if there is a correlation or not. What is more, just like the HAIS-Q methodology, phishing in combination with a questionnaire is used to validate the findings, only the other way around and with another aggregation level.

Results from case study 1	*Total employees*	*Safe feeling mean work*	*Safe feeling SD work*	*Safe feeling mean home*	*Safe feeling SD home*
1	108	7.96	1.28	6.61	1.85
2	31	7.87	1.34	6.52	2.57
3	6	8	0.33	6.67	2.56
4	2	7	4	8	1
5	5	8	0	7	0.4
6	3	8.33	0.22	6.67	0.22
7	57	7.84	2.73	6.88	2.21
8	9	7.89	0.77	6.78	3.06

Table 11: Safe acting vs safe feeling

The results as described in table 11 are the combination of the results of case study 1, as described in 4.3.4 and the results of case study 2 as described in 4.4.4. The results of case study 2 have a **confidence interval of 95%** and a **margin of error of 4%**, which means they are a good reflection of the investigated group. In general results 1-4 (overall cyber safe feeling mean work: 7.93, overall mean home: 6.61) are desirable (because they only take place at the internal network of the MoD), and results 5-8 (overall cyber safe mean work: 7.88, overall mean home: 6.86) are less desirable (because the actions leave the internal network of the MoD and take place on internet). These results reveal a cyber safe feeling does not automatically correspond to a true action and therefore contradicts the validation of the HAIS-Q methodology.

4.6 Conclusion

In the case study of the RNM, gamification of spear phishing was used, to determine if spear phishing itself can be used as CSA-level measurement method. Existing methodologies already used spear phishing exercises to validate their own measurement methods, but do not make use of the spear phishing as actual CSA-level measurement method. Also, results from the case study of the RNM were used to assess if current measurement methods, which primarily make use of questionnaires can be validated or invalidated. Combined with the literature study and expert-interviews the case study indicates current measurement methods are possibly contaminated, because they possibly get desirable or expected answers. These methods are therefore not sufficient and lack the use of basic statistical research. What is more, the case study calls the validation of current methods into question.

The case study also reveals basic statistical research can be used as proper design requirements in data collection studies to make the conclusions generalizable and valid. Probability sampling (like random sampling, to target a subset of the population) has to be used, in order to prevent sampling bias. What is more, the minimum sample group has to be calculated in order to be efficient and in order not to target to few samples. Also, the margin of error can be calculated, so the confidence interval can reveal how relevant the data found is.

As 91% of all cyberattacks are initiated through some kind of phishing attack (NCSC, 2017) a spear phishing experiment can be used to measure CSA-Levels. Surprisingly, this also in somehow indicated by the HAIS-Q methodology, which uses a phishing experiment as validation method. Therefore, the phishing experiment contemplates to be an accomplished method to prolong data from large sample groups and to identify biases.

In addition, non-validated data found indications trained employees scored worse in comparison with untrained employees. Online research revealed more studies had comparing finding, but all were unable to explain these unexpected findings. Therefore, additional research is necessary to explain these results, for example by doing a questionnaire among the targeted employees in order to explain their reactions. This can be supplemented with asking for changes in training, and asking for a score how cybersecure they feel within the MoD and at home. This might reveal explanations for these remarkable results.

As a fringe benefit, interviews with phished employees revealed more time has to be spent in the mitigation factors for phishing in the general cybersecurity awareness training of the MoD. Also, processes need to be clear, and it must be clear where you can go when dealing with a cyber-incident related question. What is more, indications were found that cybersecurity awareness training sessions need to be reoccurring in some manner, as the group which received the training more than one year ago had the worst score.

Some indications were found more officers attended the training in contrast with civilians. As the MoD is a military organization, maybe military employees go to available training sessions more often as in contrast to civilians, so this last group needs to be addressed in another manner. Also, the score of civilians was lower, so it might be a culture problem. As

mentioned earlier, this kind of studies are sensitive to cultural elements and not necessarily applicable to other organizations.

Finally, the second case study revealed employees act less cybersecure at work, then they do at home, because they are under the mistaken feeling IT security protects them against all cyber threats. This is an important finding, which has to be attended to in further training.

5 Methodology design and validation

5.1 Introduction

The previous chapters described the relation between cybersecurity and the role of CSA and existing models to measure CSA-levels. A gap in the body of knowledge was found and a case study was used in order to find if gamification could be used to resolve this gap. It was assumed a complete new method using gamification would be needed in order to measure CSA-levels of organizations, however results from the case studies revealed gamification and good design of a phishing experiment combined with data analytics can be used to supplement existing methodologies. This chapter presents a new methodology design, based on current methodologies, gamification and data analytics. With the presentation of the methodology the goal of this thesis is accomplished: *to develop a methodology for quantifying the level of cybersecurity awareness of organizations.*

5.2 Design process

The idea for a new methodology for CSA-level measurement came when it became apparent that current questionnaire based methods overlooked the necessity of measuring actual behavior instead of relying on subjects self-reporting on their hypothetical behavior. Using gamification, behavioral actions can be measured as measurable, repeatable and objective data. For example, in a phishing experiment objectives can be related to behavioral aspects. These behavioral aspects can be translated to measures, which can be transformed to numerical data. Ultimately, depending on the organizations internal security policy, these responses can also be given a weighting factor.

Findings from the case studies give a strong indication that gamification can be used to measure CSA-levels. However, as each organization has its own policies, rules, regulations and its own procedures on how to file reports, as well as its own organizational crown jewels and their associated vulnerabilities, these elements need to be translated to measurable numerical data in order to get a distinct image. For example, when gamification of spear phishing is used to measure this data, a proper ‘game’ scenario needs to be used in the accompanying email and website. Employees need to be tricked so they believe the email and website are genuine. This results in the necessity of two methodologies, one basic methodology with the goal to get a better generic understanding of the CSA-level and the other which is specifically tweaked to the organization. The latter will be described in the following paragraph.

5.3 Guidelines

The results of any measurement method, including the results of the new proposed methodology are all dependent on the type of organization, its geographical spread within the country or countries, cultural elements which can be specific to the organization, region or other factors. It has to be taken into account that when measuring CSA levels, these measurements will be dependent on a wide variety of factors including environmental factors as well as population factors. For example, just before one does make a measurement of the CSA level, the organization is hit by a massive cybersecurity attack such as, for instance, the Wannacry attack, which has been widely discussed in the media, or the CSA measurement is done while there is an ongoing nationwide cybersecurity campaign such as ‘Alert Online’, or the measurement is done just at the moment that a lot of new young employees were accepted while at the same time a lot of old employees were

retiring. It is clear that any measurement used by any method results in a timestamped snapshot of the organization under investigation with exact the sample population at that specific time of measurement. However, when certain simple statistic precautions are adhered to the sample results may be statistically generalizable for the total population, giving a good indication of how many employees of the total population would be tricked into clicking on a link in the email of a phishing campaign the timestamp can be used as baseline to which further measurements can be compared, for example to review if CSA-training has a positive effect on the CSA-level.

5.4 Resulting process model

5.4.1 Organization selection

The first step within the process model, is selecting the organization which has to be measured. The cyberspace model is not only is about technology, but has additional layers; the socio-technical layer and the governance layer (van den Berg et al. 2014). However, cyberspace does not exist without the influence the physical world has on the technical and socio-technical layer. The described layers all are intertwined and related, but they all have one common thread: the human factor, consisting of three elements behavior, knowledge and attitude. Adding this common thread to the model leads to the extended cyberspace model of vd Berg, which is presented in figure 21. In this model, the physical world is the organization under investigation and its specific elements behavioral, knowledge and attitude elements, that influence the results of the measurement are added, and which have a two-way influence, as the organization itself also has influence on behavior, knowledge and attitude of its employees.

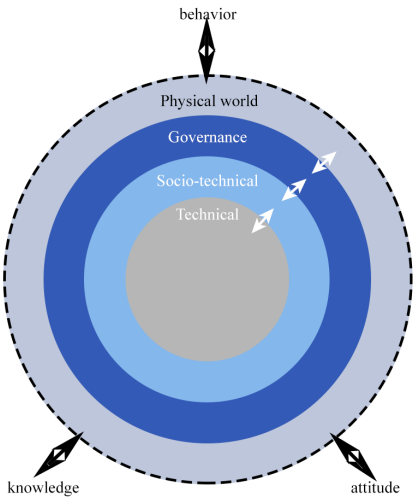


Figure 21: 3-layer cyberspace model vd Berg – extended

5.4.2 Awareness level of attention

A vital part of the new proposed methodology is the awareness training within the organization. The results of this methodology are all dependent on the awareness level of the organization. This level should be dependent on the availability of the CSA training, but the understanding of the necessity of cybersecurity and CSA training at the board level, for example to get appropriate budget, resources and mandate. This includes setting up a feedback loop after the first quantification of the CSA level is made.

5.4.3 CSA-level measurement model selection

The second step is to select a CSA-level measurement model. As earlier described in this thesis, there are several methodologies to assess the level of CSA of an organization, all of which are somehow related to behavior. The first methodology is to look if CSA is somehow part of the organization. The second methodology is to investigate how secure employees feel according to questionnaires. The third methodology is to use gamification to factual measure true behavior. These methodologies all are linked with each other: the security awareness maturity model of SANS proposed the use of a robust metrics framework, the K&K method is a metrics framework and the HAIS-Q method is a further development of the K&K method. Finally, gamification by using phishing gives us a numerical measurement of the actual behavior of employees in a cybersecurity setting. Depending on what the researcher is interested in, and how large an effort the researcher wants to make in the investigation one of these 4 methods can be selected. When the gamification of phishing is chosen, the researcher can develop the phishing 'game' in-house, or involve external parties for the phishing 'game'.

5.4.4 Basic setup

The third step, is creating a basic setup. In this scenario, it is assumed the researcher is interested in using the gamification method, which details was described in paragraph 3.5. In this case the researcher needs to setup a phishing attack to measure the CSA-level. The researcher can make use of several parties which offer this kind of service, but can also develop it internally. At this moment, it is important to define exactly what type of phishing is done, ranging from basic phishing send to a bulk population, to specific spear phishing send to specific persons only. This is an important step, because this in phishing determines the type of results and can also be seen as maturity in phishing. For simplicity, in the proposed methodology a distinction in two types of phishing is made, phishing and spear phishing. In both cases, a group needs to be targeted. In this model, a spear phishing mail send to one specific employee will only give the measurement of one subject, which would obviously be of no value whatsoever if one wanted an indication of the overall CSA of the whole. Next, dependent on what needs to be measured it is optional to use the Vishwas triad (see next paragraph) and psychological compliance factors in combination with phishing or spear phishing. A total of 8 possible combinations can be made which lead to the following phishing maturity model (figure 22).

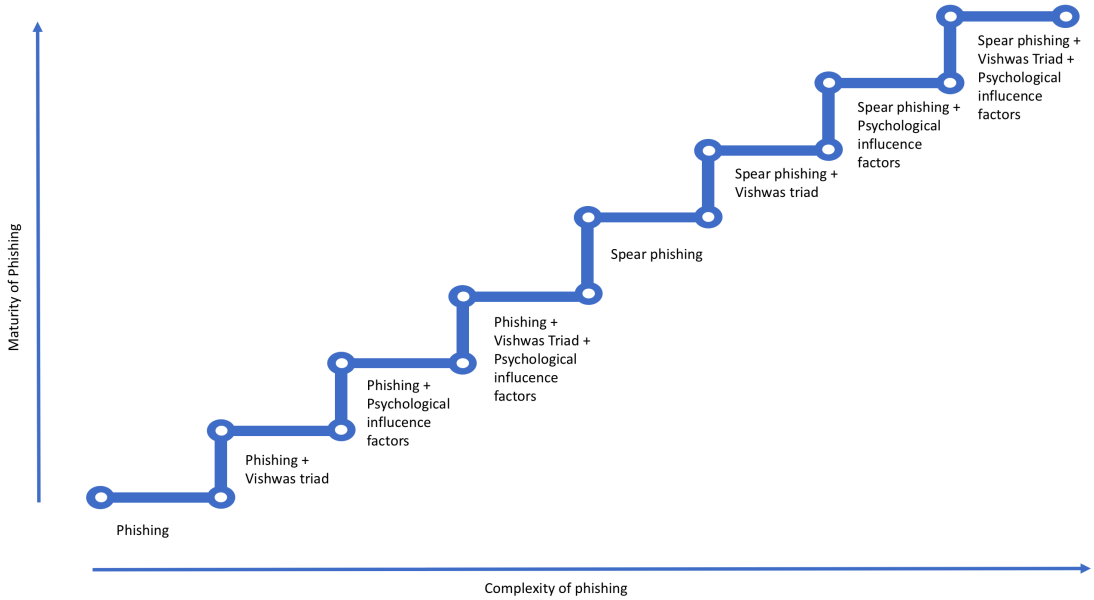


Figure 22: phishing maturity model

5.4.5 Vishwas triad

According to the Vishwas triad (Vishwanath et al. 2016), the phishing has to come from a trustworthy source (such as Google, Facebook, or internal party), has to have a field that is usually manipulated (e.g., Google documents sender name, file name, email sender's name) and needs to attack/email context which is part of the user's routine (e.g., people usually click on Google documents or click on open PDFs) or something for which they have good heuristics/thumb-rules. The basic setup needs to be aligned with the psychological compliance factors.

5.4.6 Psychological compliance factor selection

Next, psychological compliance factors used in the gamification need to be selected. This method doesn't provide templates which can be used as scenario, as these scenarios need to be adjusted for each organization. However, as shown in table 3 in paragraph 2.4.5: most scenarios used in scams use a wide variety of variations and are based on a selection of psychological influence principles: reciprocity, commitment, social validation, friendship, scarcity, authority, overloading, strong affect and diffusion of responsibility.

Depending on the organization, a selection can be made of the psychological influence factors above, however authority, reciprocity, friendship and scarcity are the most used. Using more than one influence factor results in factors reinforcing each other and is more effective than using a single factor separately.

5.4.7 Basic scientific research

The next step is to make a good design with an exact definition of the dependent variable and independent variables, and what the different experimental conditions are that you are trying to compare. Furthermore, you need to calculate the minimum needed sample size to make the results generalizable for the whole population. Using samples of the whole

population is very efficient, as not all employees need to be targeted and the researcher knows exactly how many employees need to be targeted, to get usable results. After the needed sample size is calculated, the simplest manner of sampling is random sampling meaning that random subjects of the whole population are selected until the minimum sample size number is reached. Thus, the most basic design is:

- Dependent variable: Response on phishing mail;
- Independent Variable (treatment): CSA training or no CSA training;
- Minimum sample size:

  Unlimited population: $n = \frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2}$

  Finite population: $n' = \frac{n}{1+\frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2 N}}$
- Make three equally large groups of randomly selected employees from the whole population. Give one group the CSA training, one group does not get any treatment, one group gets a safety training (no cyber content);
- Depending on the specific organizational circumstances this simple design can be varied upon;
- Now send the phishing mail to all three groups at the same time;
- Results can be collected and an analysis of the comparison of the three groups can be made.

By comparing the results of the CSA trained group to the non-trained group one can find out what the awareness training has done for the actual behavior when encountering a phishing mail. When comparing the result of CSA trained group with the safety trained group one can find out what, if any, is the contribution of giving a training as such. After analysis, the findings can be reported.

5.4.8 Execution of gamification

After all of the above steps are done, the exercise is ready to be executed. The first exercise will result in direct result of a percentage of how many employees were tricked, but can later on be used as baseline, in order to assess if the CSA program of the organization has positive effects on the CSA-level of the employees, when the gamification is repeated.

5.5 Methodology visualization

The steps presented in 5.4 result in the visualization of the methodology in figure 23.

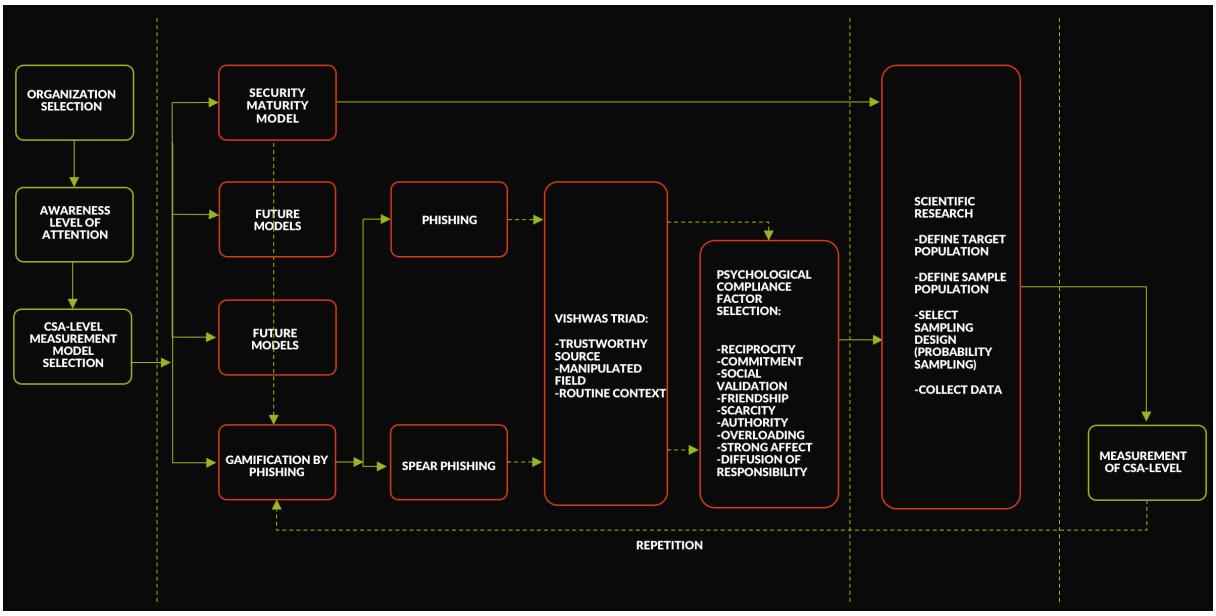


Figure 23: visualization of methodology proposal

5.6 Expert reflection

5.6.1 Introduction

In order to validate the proposed model, three peer-reviews were performed by field-experts, two internally from the MoD and one from a cybersecurity organization. The results of this peer-reviews are presented in this paragraph.

5.6.2 Positive notes

All peer-reviews agree with the usefulness of the proposed methodology[30,31,32]. The MoD uses more and more information driven operations (IDO), in which information is the enabler of those operations. By using IDO, the MoD becomes more reliable on digital information, so there are greater risks in losing the information. This can be partially mitigated by a proper CSA training. In addition, results of gamification can benefit the IDO, by providing additional measurement instruments[33]. CSA is the 'neglected child' of the MoD. Due to the lack of central coordination, the operational commands all have their own CSA agenda. Recent events and threats like the Wannacry and NotPetya ransomware attacks forces the MoD to face the facts. CSA is now on the strategical agenda of the Defence Cyber Platform, in which the Defence Security Authority has the leading role.

The proposed framework is powerful, as gamification results are a direct measure of the actual behavior of employees. Gamification is often underestimated and contributes to increasing CSA of an organization and can also be used as input for CSA training[34,35]. The proposed framework forces an organization to improve its CSA training, measurement and level. Repetition of gamification is an essential aspect in this method, because of the passage

[30] Security Company 2 (2017) Peer-review on methodology [Personal interview]
[31] Advisor DefCERT (2017) Peer-review on methodology [Personal interview]
[32] Advisor CIO Office MoD (2017) Peer-review on methodology [Personal interview]
[33] Advisor CIO Office MoD (2017) Peer-review on methodology [Personal interview]
[34] Advisor CIO Office MoD (2017) Peer-review on methodology [Personal interview]
[35] Advisor DefCERT (2017) Peer-review on methodology [Personal interview]

of employees, renewal of used IT-systems and renewal of cyber-attacks including social engineering[36].

5.6.3 Constructive criticism

The proposed methodology can be useful for the MoD, however a more constructive investigation on the implementation of the methodology within the MoD is advisable[37]. Furthermore, the proposed methodology only uses phishing as gamification method. In additional research other gamification methods, like USB-stick drops, canary tokens and password cracking should be investigated to complement the methodology[38]. The feedback loop to the CSA training can be further specified[39,40]. In order for the methodology to be useful it is important to have specific scenarios developed for each organization, this could be a showstopper for organizations to implement the methodology as this will take time and money. Also, a distinction needs to be made between different types of phishing[41]. In the specific MoD scenario, an additional scenario needs to be researched in further studies: military operations on military operational networks not connected to the regular internet. It is likely the 'phishing measurement method' will not work, however this can be possibly circumvented by using the earlier mentioned other gamification methods[42].

5.6.4 Conclusion of the peer-review criticism

Peer-reviews revealed the potential of the proposed methodology and applicability within organizations. The distinction of different types of phishing was added to the proposed model in 5.4, which resulted in the phishing maturity model presented in figure 22.

5.7 Conclusion

This chapter discussed how CSA-levels of organizations can be measured and proposed a quantitative measurement methodology of actual behavior as part of a gamification method. The results of any measurement methods, including the results of the new proposed methodology are all dependent on the type of organization, its geographical spread within the country or countries, cultural elements which can be specific to the organization, region or other factors. When conducting the research with a solid research design, the advantage is it can be performed more efficient, and even more important the results are more reliable and generalizable for the whole organization. Using the new methodology, which is built on top of existing models as addition, it can support organizations in the measurement of their CSA-level. As the above methodology is constructed after the case study at the RNM was performed, it is only validated using peer-reviews and needs to be verified in future research.

[36] Advisor DefCERT (2017) Peer-review on methodology [Personal interview]
[37] Advisor CIO Office MoD (2017) Peer-review on methodology [Personal interview]
[38] Advisor DefCERT (2017) Peer-review on methodology [Personal interview]
[39] Security Company 2 (2017) Peer-review on methodology [Personal interview]
[40] Advisor DefCERT (2017) Peer-review on methodology [Personal interview]
[41] Security Company 2 (2017) Peer-review on methodology [Personal interview]
[42] Advisor DefCERT (2017) Peer-review on methodology [Personal interview]

6 Conclusion and recommendations

6.1 Conclusion

The goal of this thesis was to develop a methodology for quantifying the level of cybersecurity awareness of organizations based on the measurement of actual behavior. It was the assumption the new methodology had to be a stand-alone methodology, however this thesis revealed the methodology can be used on top of and in addition to already existing CSA-level measurement methods. The problem upon now, however, was that these methodologies were not combined into one usable methodology. The new usable methodology that has been developed to help organizations measure their CSA-level, although primarily based on existing methodologies does not suffer from that defect. All steps in the new methodology are described, and all steps are based on the results of the research reported in this thesis. As the above methodology was constructed after the case study at the RNM was done, it is not yet validated and it needs to be validated by future research.

In this thesis, the MoD/RNM was used as case study, which is not necessarily relevant to all kind of organizations. The MoD/RNM is a unique organization, with unique organizational and cultural aspects which operate in security and law enforcement with a unique population of employees, both military as civilians. Although the organization itself is not a very representative one, many findings that are made with the case studies are applicable in general business organizations.

6.2 Recommendations

Future research is necessary and the proposed methodology, which was a result of the research performed, needs to be further elaborated and tested. A limitation of this study is the degree in which the results of the experiment would be the same when the experiment would be conducted in other type of organizations or even the same type of organizations in other countries or within different cultures. It is therefore recommendable to conduct this experiment in multiple type of organizations in different cultures to provide more reliable data and to validate these findings.

In future research, it is recommended to think ahead when designing an experiment, by carefully choose the variables that one wants to experimentally vary and for which one tries to measure their influence on their dependent variable(s). Besides including a control group whenever possible, it pays off to calculate beforehand the minimum needed number of subjects to get some reliable results, as this obviously can have some budgetary consequences. With all the modern data science techniques available today, it is very helpful to enrich a sparse experimental dataset with additional data. Nowadays there is a lot of this additional data available in most organizations. When one is allowed to use this data, combining this with the experimental can result in a Big Data or Data Analytics exercise (which is called intelligence-led action within the RNM). The more you spend time on executing your data science and data analysis, the more leads you may find to conduct your research. No research is performed perfectly, the more data you have on actual behavior, the more realistic your models will be.

Non-validated data found indications trained employees scored worse in comparison with untrained employees. Online research revealed more studies had comparing finding, but all

were unable to explain these unexpected findings. Therefore, additional research is necessary to explain these results, for example by doing a questionnaire among the targeted employees in order to explain their reactions.

7 Bibliography

Advisory council on international affairs, 2011. Cyber Warfare. *Cyber Warfare*, (77), pp.1–18.

Alert Online, 2017. Nederlander nonchalant met cybersecurity op werk. Available at: https://www.alertonline.nl/nieuws/2017/nederlander-nonchalant-met-cybersecurity-op-werk [Accessed November 5, 2017].

Baarda, T.A. Van & Verweij, D.E.M., 2006. *Military Ethics: The Dutch Approach : a Practical Guide*, Martinus Nijhoff Publishers.

Belaissaoui, H. & Elkhannoubi, M., 2015. A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification. In *15th International Conference on Intelligent Systems Design and Applications (ISDA)*. Marrakech, pp. 1–6.

van den Berg, B., 2017. Actors and behaviours in cyberspace: Introduction.

van den Berg, J. et al., 2014. On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. *NATO STO/IST-122 symposium in Tallin*, (c), pp.1–10.

van den Berg, J., 2015. Wat maakt cyber security anders dan informatiebeveiliging ? *Magazine nationale veiligheid en crisisbeheersing*, 2, pp.4–5.

Brecht, D., 2015. Security awareness and spear phishing: How to stay out of danger. Available at: http://www.appstechnews.com/news/2015/aug/24/security-awareness-and-spear-phishing-how-stay-out-danger/ [Accessed May 1, 2017].

Burtner, W.K., 1991. Hidden Pressures. *Notre Dame Magazine*, pp.29–32.

Butavicius, M., Mccormac, A. & Zwaans, T., 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further. *Computers & Security*, 66, pp.40–51. Available at: http://dx.doi.org/10.1016/j.cose.2017.01.004.

CCDCOE, 2017. Cyber Definitions. Available at: https://ccdcoe.org/cyber-definitions.html [Accessed October 5, 2017].

Cialdini, R.B., 2001. *Influence: Science and Practice*,

Commision on enhancing national cybersecurity, 2016. Report on securing and growing the digital economy.

Cyber Security Academy, 2017. Glossary. Available at: https://www.csacademy.nl/en/glossary [Accessed October 5, 2017].

Darkreading.com, 2017. Phishing Emails that Invoke Fear, Urgency, Get the Most Clicks. Available at: https://www.darkreading.com/endpoint/phishing-emails-that-invoke-fear-urgency-get-the-most-clicks/d/d-id/1330100 [Accessed October 13, 2017].

Defensie.nl, 2017. Organisation marechaussee. Available at: https://www.defensie.nl/english/organisation/marechaussee/organisation [Accessed September 30, 2017].

Deterding, S., 2011. Gamification : Toward a Definition. , pp.12–15.

Dodge, R.J., Carver, C. & Ferguson, A.J., 2007. Phishing for user security awareness. , 26, pp.73–80.

Ducheine, P.A.L. & Voetelink, J.E.D., 2011. Cyberoperaties : naar een juridisch raamwerk. *Militaire spectator*, (6), pp.3–6.

Engel, G., 2014. Deconstructing The Cyber Kill Chain. Available at: http://www.darkreading.com/attacks-breaches/ deconstructing-the-cyber-kill-chain/a/d-id/1317542 [Accessed May 10, 2017].

ENISA, 2015. *Definition of Cybersecurity - Gaps and overlaps in standardisation*,

ENISA, 2016. Review of Cyber Hygiene practices. , (December).

ESET, 2017. Free ESET Cybersecurity Awareness Training. Available at: https://www.eset.com/us/cybertraining/ [Accessed October 5, 2017].

F-Secure, 2017. F-Secure State of cyber security. Available at: http://images.news.f-secure.com/Web/FSecure/%7Bd52f77ef-dd23-4871-ab9b-2ae794f4dadd%7D_F-Secure-Threat-Report-State_of_Cyber_Security_2017.pdf.

Fink, G. et al., 2013. Gamification for Measuring Cyber Security Situational Awareness BT - Foundations of Augmented Cognition: 7th International Conference, AC 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013. Proceedings. In D. D. Schmorrow & C. M. Fidopiastis, eds. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 656–665. Available at: https://doi.org/10.1007/978-3-642-39454-6_70.

Forbes, 2014. Security Experts At RSA Decry Government Hacking. Available at: https://www.forbes.com/sites/larrymagid/2014/02/25/security-experts-at-rsa-conference-decry-government-hacking/#348237355e1b [Accessed September 30, 2017].

Fox-IT, 2017. Search. Available at: https://www.fox-it.com/nl/zoeken/?q=cybersecurity&submit= [Accessed October 6, 2017].

Furnell, S.M., Jusoh, A. & Katsabas, D., 2005. The challenges of understanding and using security : A survey of end-users. , 5, pp.27–35.

Gragg, D., 2002. A Multi-Level Defense Against Social Engineering. , p.18. Available at: https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920.

Grøtan, T.O., 2014. Hunting high and low for resilience : Sensitization from the contextual shadows of compliance. *Safety, Reliability and Risk Analysis: Beyond the Horizon*, (2001), pp.327–334.

Gulati, R., 2003. The Threat of Social Engineering and Your Defense Against It. *Information Security*, pp.1–15. Available at: https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232.

Harl, 1997. People Hacking : The Psychology of Social Engineering. *Text of Harl's Talk at Access All Areas III*.

Hennis-Plasschaert, J.A., 2014. *Kamerbrief over Offensieve cybercapaciteit Defensie*, Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/03/17/kamerbrief-over-offensieve-cybercapaciteit-defensie.

Heuer, R.J., 1999. *Psychology of Intelligence Analysis*,

ISO, 2016. ISO / IEC 27000:2016. , 2016.

Jung, N. et al., 2014. How emotions affect logical reasoning : evidence from experiments with mood-manipulated participants , spider phobics , and people with exam anxiety. , 5(June), pp.1–12.

Kaspersky, 2017. Kapsersky Security Awareness. Available at: https://www.kaspersky.nl/enterprise-security/cybersecurity-awareness [Accessed October 5, 2017].

Kearney, W. et al., 2017. Phishing and Organisational Learning To cite this version : , pp.0–12.

Khan, B. et al., 2011. Effectiveness of information security awareness methods based on psychological theories. , 5(26), pp.10862–10868.

Koroliov, V., Turesson, M. & Brolin, O., 2009. *What is your password?* JÖNKÖPING

UNIVERSITY.
Kruger, H., Drevin, L. & Steyn, T., 2006. A framework for evaluating ICT security awareness.
Kruger, H. & Kearney, W., 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(4), pp.289–296.
Lockheed Martin, 2011. The Cyber Kill Chain. Available at: http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html [Accessed September 25, 2017].
Macdougall, S., 2012. Social Engineering Threats and Countermeasures In An Overly Connected World. Available at: https://media.blackhat.com/ad-12/MacDougall/bh-ad-12-social-engineering-threats-MacDougall-Slides.pdf.
McCormac, A. et al., 2016. Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q). , pp.1–10.
MediaPro, 2017. Cyber Security Awareness Training. Available at: https://www.mediapro.com/courses/cyber-security-awareness-training/ [Accessed October 5, 2017].
Ministry of Defense, 2017. ABDO 2017.
Ministry of Defense, 2012. *Defensie cyber strategie*, Available at: https://www.rijksoverheid.nl/documenten/brochures/2012/06/27/brochure-defensie-cyber-strategie.
Ministry of Defense, 2015a. Defensie High-Level IT-ontwerp. , p.77.
Ministry of Defense, 2016a. *Kamerbrief - Voortgangsrapportage uitvoering Defensie Cyber Strategie*, Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2016/03/15/kamerbrief-over-de-uitvoering-defensie-cyber-strategie.
Ministry of Defense, 2015b. Kerngegevens Defensie - Feiten en cijfers.
Ministry of Defense, *Veiligheidsonderzoeken bij Defensie en defensieorderbedrijven*,
Ministry of Defense, 2016b. Zijn onze digitale dijken hoog genoeg? Available at: https://magazines.defensie.nl/defensiekrant/2016/25/digitale-dijken [Accessed February 18, 2017].
Mitnick, K.D. & Simon, W.L., 2003. The Art of Deception: Controlling the Human Element in Security. *BMJ: British Medical Journal*, p.368. Available at: http://www.bmj.com/content/347/bmj.f5889.
Mourik, D. Van, 2017. Targeted attacks and the human vulnerability.
Mouton, F. et al., 2014. Social Engineering Attack Framework. *Information Security for South Africa*, pp.1–9.
Munnichs, G., Kouw, M. & Kool, L., 2017. Een nooit gelopen race. , p.86.
Mylonas, A., Kastania, A. & Gritzalis, D., 2012. Delegate the smartphone user ? Security awareness in smartphone platforms. *Computers & Security*, 34, pp.47–66. Available at: http://dx.doi.org/10.1016/j.cose.2012.11.004.
National Cyber Security Centre, 2016. Cyber Security Assessment Netherlands 2016.
National Cyber Security Centre, 2017. Cyber Security Beeld Nederland 2017.
Ncalculators.com, Random Sampling Error Calculator, Formula, Example Calculation. Available at: https://ncalculators.com/statistics/margin-of-error-calculator.htm [Accessed December 1, 2017].
NCTV, 2017. Alert Online. Available at: https://www.alertonline.nl [Accessed June 1, 2017].
NEN, 2012. NEN-ISO/IEC 31010:2009.
NIST, 2017. Framework for Improving Critical Infrastructure Cybersecurity. , 1.1.

NIST, 2003. SP800-50 Building an Information Technology Security Awareness and Training Program. , (October).
NIST, 2014. Special Publication 800-16 A Role-Based Model for Federal Information Technology / Cybersecurity Training.
Norrie Johnston Recruitment, 2017. Cyber Security - How real is the threat and how can you reduce your risk?
Parsons, K., McCormac, A., Pattinson, M., et al., 2014. A study of information security awarness in Australian government organisations. *Information Management & Computer Security*, pp.334–345.
Parsons, K., McCormac, A., Butavicius, M., et al., 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaires (HAIS-Q). *Computers & Security*, 42, pp.165–174.
SANS, 2017a. Cyber Security Trends : Aiming Ahead of the Target to Increase Security in 2017.
SANS, 2016a. Human Metrics: measuring behavior. Available at: https://securingthehuman.sans.org/media/resources/presentations/STH-Presentation-HumanMetrics.pdf [Accessed September 19, 2017].
SANS, Information Security Resources. Available at: https://www.sans.org/information-security/ [Accessed July 26, 2017a].
SANS, 2014. Killing Advanced Threats in Their Tracks : An Intelligent Approach to Attack Prevention. , p.17.
SANS, SANS Phishing Training. Available at: https://securingthehuman.sans.org/security-awareness-training/phishing [Accessed November 24, 2017b].
SANS, 2017b. Security awareness report.
SANS, 2016b. Security Awareness Report.
SANS, 2004. Social Engineering: Information Bandits. Available at: http://zma.es/Incident Handler/real-world-arp-spoofing/real-world-arp-spoofing_487.pdf.
Shipley, D., 2017. Hacking cars: cybersecurity regulations needed for new vehicles. Available at: http://www.cbc.ca/news/canada/new-brunswick/cybersecurity-hacking-cars-david-shipley-opinion-1.4206548 [Accessed July 19, 2017].
Staf Commandant KMar, 2015. A3-jaarplan 2016 Koninklijke Marechaussee. , p.2016.
Stanton, J.M. et al., 2005. Analysis of end user security behaviors *. , pp.124–133.
Surveymonkey.com, Sample Size Calculator. Available at: https://www.surveymonkey.com/mp/sample-size-calculator/ [Accessed December 1, 2017].
Symantec, 2016. Internet Security Threat Report. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [Accessed September 7, 2017].
Teplow, L., 2017. Breaking Down the Dangers of Social Engineering. Available at: https://www.continuum.net/blog/breaking-down-the-dangers-of-social-engineering [Accessed November 22, 2017].
University of California Santa Cruz, 2017. Security Awareness Training. Available at: https://its.ucsc.edu/security/training/index.html%0D [Accessed October 5, 2017].
University of Minnesota, 2015. Introduction to Psychology.
University of Victoria, LAB 3: Sampling Methods. Available at: http://labs.geog.uvic.ca/geog226/frLab3.html [Accessed November 4, 2017].
Vishwanath, A. et al., 2011. Why do people get phished? Testing individual differences in

phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, (51), pp.576–586.
Vishwanath, A., Harrison, B. & Ng, Y.J., 2016. Suspicion , Cognition , and Automaticity Model of Phishing Susceptibility.
Volkskrant, 2016. Hennis: dreiging cyberspionage tegen Defensie neemt toe. Available at: http://www.volkskrant.nl/media/hennis-dreiging-cyberspionage-tegen-defensie-neemt-toe~a4263755.
WarLord, 2016. Six Ways to Automate Metasploit. Available at: http://hackingandsecurity.blogspot.nl/2016/05/six-ways-to-automate-metasploit.html [Accessed November 22, 2017].
Weathington, B.L. et al., 2011. Applied Psychology in Everyday Life.
Wikileaks, Vault 7: CIA Hacking Tools Revealed. Available at: https://wikileaks.org/ciav7p1/cms/index.html [Accessed May 1, 2017].
Wilson, M., Hash, J. & Division, C.S., 2003. Building an Information Technology Security Awareness and Training Program. *NIST Special Publication 800-50*, (October).
Workman, M., 2007. Gaining Access with Social Engineering : An Empirical Study of the Threat Gaining Access with Social Engineering : An Empirical Study of the Threat. *Information Systems Security*, 16, pp.315–331.
Zanna, M.P., 1991. *Advances in Experimental Social Psychology*,
Zichermann, G. & Cunningham, C., 2011. *Gamification by Design*,