NTNU

Norwegian University of
Science and Technology

Use of Gamification in Security Awareness and Training Programs

Eyvind Garder B Gjertsen

Master of Science in Communication Technology
Submission date: June 2016
Supervisor: Maria Bartnes, ITEM
Co-supervisor: Waldo Rocha Flores, Ernst & Young AS
Erlend Andreas Gjære, SINTEF

Norwegian University of Science and Technology
Department of Telematics

Title: Use of Gamification in Security Awareness and Training Programs

Student: Eyvind Garder Bull Gjertsen

Problem description:

Several independent reports reveal that "the human factor" is the primary cause for a large number of IT security breaches. IT security awareness and training programs have been implemented to rectify this issue, however, these programs have previously been viewed as tedious and superfluous and thus failed to prepare employees for potential cyber security attacks.

Gamification, commonly defined as "the use of game design elements in non-game contexts", has previously shown promise in creating engaging and productive learning environments, in both education and business contexts. Some research has been dedicated to the connection between security awareness training and gamification, though only focusing on the effects of short-term implementations of such programs. Other limitations of current research include a classification of the most effective attributes of gamification to be used in the training.

Following a qualitative research approach, the main goal of this thesis will be to determine if – and possibly how – gamification may be applied in a long-term continuous program in order to improve learning outcomes and affect user behaviour. The methods used will involve interviews with security specialists and discussions with user groups in order to assess the feasibility and usability of a conceptual software application.

Responsible professor: Maria Bartnes, ITEM

Supervisors: Waldo Rocha Flores, Ernst & Young AS

Erlend Andreas Gjære, SINTEF

Abstract

The security reports are unambiguous: the human factor constitutes a real vulnerability in the information security domain. It is crucial that employees of companies and governments understand the risks and threats connected with use of IT systems, and act on the knowledge to prevent security breaches and leakage of sensitive information to cyber criminals or nation state espionage. It is assumed that security awareness and training programs are one of the primary ways of raising someone's conciousness and building competence in the field of information security. However, current programs are sometimes viewed as tedious and uninteresting by the employees that take them. Consequently, the programs fail to create the behaviour and competence needed for employees to anticipate and prevent security breaches.

Gamification is a design technique where elements from games are deployed in non-game contexts to increase user engagement and motivation. This thesis has taken a qualitative research approach to assess if and how gamification can be used in security awareness and training programs in order to defeat the tediousness and thus improve learning outcomes. The idea that has been studied is a long-term, continuous program that makes use of a gamified software application to mediate awareness and training material to employees. Qualitative data has been collected through interviews with security professionals and workshops with end users from two different Norwegian companies, in order to gain an understanding of the possibilities and limitations of the proposed concept. A prototype of a gamified application was developed to aid the research.

The results indicate that gamification can have positive effects in combination with security awareness and training. Firstly, it was found that companies and employees often can have multiple common ambitions connected with the training; common goals that should be used as focus points in future programs. Secondly, it was discovered that employees would principally value factors such as progression and mastery as motivational stimulus in the training. Thirdly, results from the workshops suggests that gamification can increase motivation towards completing training, and potentially improve learning outcomes as a result of this. Conclusively, it was indicated that a long-term gamified training program, with use of short and concise exercises, could lead employees to think more about security during the daily work, which in turn suggests a potential for behaviour change.

Sammendrag

Flere uavhengige sikkerhetsrapporter varsler at den menneskelige faktoren potensielt utgjør en stor trussel for informasjonssikkerheten i både privat og offentlig sektor. Det er kritisk i dagens samfunn at alt personell er kjent med de ulike farer og trusler som følger med bruk av IT-systemer, samt gjennomfører opplæring i hvordan å identifisere og avverge angrep og lekasjer av sensitiv informasjon til kriminelle og annen industriell spionasje. Bevisstgjørings- og opplæringsprogrammer anses som en av de fremste metodene for å bygge nødvendig kompetanse hos ansatte. Problemet med dagens programmer er at de ofte oppfattes som kjedelige eller uinteressante. Derfor mislykkes mange programmer med formålet sitt å økte bevissthet og kompetanse blant ansatte til å håndtere sikkerhetstrusler.

Spillifisering (eng. "gamification") er en designmetode som nyttiggjør spillelementer i sammenhenger som ikke i utgangspunktet har noe med spill å gjøre, for å øke brukeres engasjement og motivasjon. Studien som presenteres her, har gjennom kvalitative forskningsmetoder undersøkt hvorvidt spillifisering kan brukes som et virkemiddel i sikkerhetsopplæringen for å unngå kjedsomhet, og bidra til forbedringer i læringsutbyttet blant programtakerne. Studien tar utgangspunkt i en idé som omfatter et langtids, kontinuerlig opplæringsprogram, hvor kjernekomponenten er en spillifisert programvareapplikasjon. Kvalitative data har blitt samlet gjennom intervjuer med sikkerhetseksperter, samt workshops med sluttbrukere hos to norske selskaper, for å få en forståelse av hvilke muligheter og begrensninger en slik løsning fører med seg. En prototype har også blitt utviklet for å støtte forskningen.

Resultatene peker i retning av at spillifisering vil ha positive innvirkninger på opplæringen. Gjennom datainsamlingen ble det funnet at bedrifter og ansatte gjerne kan ha flere felles mål og interesser koblet til treningen, slik at man bør fokusere på disse målene når man utarbeider opplæringsprogram. Det ble også funnet at ansatte verdsetter bruk av elementer som progresjon og mestring for å øke motivasjon. Resultatene fra workshop-ene indikerer at spillifisering vil øke motivasjonen til å gjennomføre treningen, og på så måte bidra til å bedre læringsutbyttet. Avslutningsvis ble det antydet at et langtids opplæringsprogram, med bruk av korte og konsise oppgaver, kan lede ansatte til å tenke mer på sikkerhet i det daglige arbeidet, noe som indikerer et potensiale for atferdsendring.

Preface

This thesis marks the conclusion of my Master's degree in the Communications Technology program at the Norwegian University of Science and Technology. It has been five challenging, yet very exhilarating years.

I would like to thank my supervisors Waldo Rocha Flores and Erlend Andreas Gjære, and responsible professor Maria Bartnes for invaluable help and guidance during this thesis project.

I would also like to thank the interviewees and workshop participants (who shall remain anonymous) for taking part in this study, and for sharing their ideas, views and opinions.

Contents

List of Figures

List of Tables

List of Acronyms

API Application Programming Interface.

DSRP Design Science Research Process.

ENISA European Union Agency for Network and Information Security.

IT Information Technology.

NIST National Institute of Standards and Technology.

SaaS Software as a Service.

SAT Security Awareness and Training.

SDT Self-Determination Theory.

USB Universal Serial Bus.

WP Workshop Participant.

Chapter 1
Introduction

"What is fascinating—and disheartening—is that over 95 percent of all incidents investigated recognize *human error* as a contributing factor."
IBM [2014] Cyber Security Intelligence Index

Weak passwords, social engineering attacks, system misconfiguration, unsecured wireless networks—the list goes on; they are factors that encompass the human aspect of information security. A common misconception that people tend to have, is that security controls and technology will automatically protect against cyber threats [Symantec, 2016]. In many cases it really comes down to the human as the last line of defence. The 2015 security report from Check Point Security informed that 60% of all recorded attacks now were directly targeted against client endpoints, which was an increase of 28% from 2014 [Check Point, 2015]. Symantec [2016] reported that spear-phishing campaigns, especially targeting employees, increased with 55% in 2015. Moreover, Microsoft [2015] announced that attackers have relied increasingly on social engineering to spread malware and compromise systems. Check Point [2015] said the perception is that it actually takes less effort to compromise a network via the client side, because "humans are much easier to dupe than machines". It was also stated that the client side is where you often would find poor security practices and insufficient protection.

EY's Global Information Security Survey of 2015, revealed that "careless or unaware employees" was ranked as the overall top vulnerability by the 1,755 participating organisations [EY, 2015]. The Norwegian Information Security Forum's (ISF) 2015 member survey concluded that the most important focus for security among the respondents in 2016 would be "increase of awareness and training for employees". One respondent disclosed that "95% of all attacks on us are through email" [ISF, 2015]. Evidently—as signalled by IBM [2014]—"it is important to educate employees on an ongoing basis about identifying suspicious communications and potential risks to the organisation".

1.1 Problem

Security breaches involving employees are generally caused by two main issues: (1) low motivation to follow guidelines and policies because it tends to slow down work processes, or (2) lack of awareness, knowledge, and ability to recognize and intercept threats and attacks [NSM, 2015]. Efforts made to tackle these issues include the implementation of Security Awareness and Training (SAT) programs. The purpose of a SAT program is to focus attention on security, explain rules and proper behaviour for use of IT systems, and produce the skills and competence the employees need to work securely [NIST, 2003]. However, based on the reports that show high numbers of security breaches linked to human error, the assumption is that current SAT programs are—to some extent—failing to accomplish their goal. Examples of obstacles connected with current programs include: the lack of engaging materials, that they are too rare and narrow, and that some employees would in fact consider security training as "a waste of time" [Leach, 2003; Winkler and Manke, 2013].

1.2 Assignment

The purpose of this thesis is to consider an alternative approach to SAT. More specifically, the task is to assess whether the use of *gamification* can help to create a more engaging and educational environment for SAT programs. Table 1.1 gives three research questions that have been selected as the scope for the study. The first two questions are worked out in accordance with the gamification literature that is presented in Chapter 2.

Table 1.1: Research questions.

1	How can good security behaviour be viewed as an advantage in the eyes of the employee?
2	Which motivational factors are the most important in a security awareness and training program?
3	What are the possibilities and limitations of a long-term, gamified security awareness and training program?

A qualitative research approach has been taken to address the research questions and assess the usability and feasibility of a gamified SAT program. The methods used for data collection include interviews with security professionals and workshops with end users. Additionally, based on the research results, a prototype has been developed to demonstrate a gamified training application.

1.3 Terminology and Definitions

In the context of this thesis, the term *security* is used as a direct reference to *information security*, i.e. the protection of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption [SANS, 2016]. There is also some ambiguity in the use of the terms security *awareness* and security *training*, and what their purposes are [Tsohou et al., 2008]. In this study, a SAT program is thought of as an ingredient in the shaping of an organisation's *security culture*—the organisation's security capacity as represented by the employees' knowledge, motivation, posture, and behaviour [NSM, 2016].

Furthermore, the definition of gamification is not entirely clear-cut, as it tends to differ slightly in terms of phrasing and broadness in various publications. In this thesis, it refers to *the use of game design elements in non-game contexts*, as defined by Deterding and Dixon [2011]. Typically, gamification involves the adoption of game design techniques and game mechanics in order to change behaviour, develop skills, or drive innovation among a target audience—that be employees, customers, or a community [Burke, 2014].

1.4 Report Outline

The rest of the report is structured as follows:

Chapter 2 conducts a review of past studies on security awareness and training, explores the elements of gamification, and concludes with a brief review of two previous studies on the use of gamification in SAT.

Chapter 3 introduces this study's proposed use of gamification in security awareness and training, along with the prototype that has been developed.

Chapter 4 details the research method, and explains how the interviews and workshops were implemented.

Chapter 5 presents the results from the data collection.

Chapter 6 leads a discussion on the research results and the prototype in attempt to answer the research questions.

Chapter 7 draws the conclusion of the study and projects future work.

Chapter 2
Background

This chapter reviews some of the existing literature in the field of security awareness and training, and gamification. The goal of the chapter is to identify potential ties between the challenges, proposed solutions, and best practices for SAT, and the problems that gamification is known to solve. The chapter concludes with a review of previous studies on the use of gamification in SAT.

Relevant literature The method used to find relevant literature on SAT consisted largely in searches on Google and Google Scholar[1]. The search phrases used were "security awareness", "security training", "gamification", and "security awareness (plus) gamification". Results were evaluated according to topic and abstract. Browsing was continued until the topics no longer seemed applicable; after approximately 5-10 pages of results. Relevant literature was also found through citations. Appropriate gamification design frameworks were found through searches in the University's online library.

2.1 Security Awareness and Training

Here is a classical example: a company utilises a said system to manage confidential information. The security is top notch; state-of-the-art firewalls repel unauthorised access and all known attack vectors; the authentication protocols are based on industry standards; all communication is encrypted with strong keys. Employees access the system with a username and password. An employee receives an e-mail from someone claiming to be from the IT department, asking for their login information in connection with some important system management event. What does the employee do? The scenario is only one of numerous scenarios where the employee is in a unique position to either cause or prevent a security breach. Even if the system security is cutting edge, a simple mistake can paralyse every available security mechanism.

[1] Google Scholar; `https://scholar.google.com`; "Stand on the shoulders of giants".

2.1.1 Challenges

Security is typically one of those things in life, that, if you do everything right, noting happens. There are no (tangible) positive outcomes; no pat on the back. It is only when a mistake is made that reactions emerge—usually negative reactions. At the same time, good security behaviour does not explicitly make people better or more effective at doing their jobs; sometimes it is actually the opposite. Consequently, employee security behaviour and training can become a struggle for the security management.

NIST [2003] accentuates the importance of taking a step-by-step approach to the construction of security competence in order to change behaviour or reinforce good security practices. Shaw et al. [2009] outlined three distinct states of awareness, or competence, that need to be considered when developing a SAT program: perception, comprehension, and projection. Firstly, it is important to make sure that recipients have an elementary conception of what security is, such that they are able to perceive the importance and relevance of having a focus on information security. Secondly, one must ensure that learners are able to comprehend the actual purpose of the content—that the potential risks give meaning and are inherent to the learners. Thirdly, the goal of a SAT program is ultimately to affect employee behaviour towards security policy compliance. Will the learner acknowledge the policies and adjust their behaviour to follow them, after completing the training?

Behaviour change is a precarious subject and is actually more a case of psychology than of security itself [Tsohou et al., 2015; Bada et al., 2015]. The first thing to acknowledge is that people are different—and somewhat unpredictable. This affects both how people regard security in general, as well as how they will respond to security training. Tsohou et al. [2015] provided an aggregated list of factors that have been mentioned in extant literature to affect security policy compliance. The list is reproduced in Table 2.1. Seemingly, there are several factors to consider other than just sheer awareness. For example, people may have different opinions as to "how big a risk actually is" when it comes to security breaches or attacks. If the *perceived risk of a security breach* is low, one might not be as mindful to enact according to the security policies. Other factors, such as *benefit versus cost of compliance* and *work impediment*, may lead people to diverge from compliance because the efforts of acting securely are considered too much of an inconvenience. Moreover, some people may in fact doubt their *self-efficacy* in that they are unequipped to handle security related issues. Tsohou et al. [2015] said that these factors come as a result of "cognitive and cultural biases" that people may have, based on their personal beliefs and experiences. A natural question to ask here is then; how is it possible to influence such biases?—And more importantly, are SAT programs capable of such a task?

Table 2.1: Factors affecting compliance. Replicated from Tsohou et al. [2015].

Factors affecting information security policy compliance
Information security awareness
Cost of compliance/response cost
Benefit of compliance
Cost of non-compliance
Safety of resources achieved by compliance
Work impediment
Perceived severity and perceived certainty of sanctions
Perceived probability and perceived severity of security breach
Perceived vulnerability
Response efficacy
Self-efficacy
Social pressure/normative beliefs
Habit

2.1.2 Current Research

Fortunately, a substantial amount of research has been dedicated to the relations between security awareness and training, and psychology. Consequently, there are multiple suggestions and recommendations available on how to account for the psychological aspects of awareness and policy compliance when building SAT programs.

Explain why Siponen [2000] said it is "extremely important" to always provide an explanation of why security policies and guidelines are the way they are. It will have a significant motivational impact on the employees if a logical and relevant reasoning underlines the policies and regulations.

Focus on the employee Expanding on this, Puhakainen and Siponen [2010] proposed a new approach to SAT based on constructivism, a teaching method where two-way communication is a leading principle. The approach was tried in an 11-month action research study including 16 people from a Finnish technology company. The key findings of the study were:

- Training material should be communicated in ways that will trigger cognitive processing of the information, which will cause longer-lived memory and ownership of the knowledge.
- Learning tasks should be of personal relevance to the recipients.

- Learning tasks should account for previous knowledge.
- Security communication should be integrated with normal business communication, to show that security is an important component in the normal work and business activities.
- Security communication should be a continuous activity rather than a periodic one.

Include the employee In a similar study, Albrechtsen and Hovden [2010] proposed a solution to use "local employee participation, collective reflection and group processes" as an improved learning process for employees. In an intervention study, security workshops with groups of 10-15 participants were held with measurements of knowledge before and after. It was discovered that awareness did in fact have a significant increase among the relevant employees, and that it remained inherent for at least six months. It was concluded that employees felt more motivated by the alternative way of attending to security. The results would suggest that more personalised, user-centric, and collaborative platforms are propitious for SAT programs.

Take advantage of technology Shaw et al. [2009] determined in an experimental study that there are positive correlations between the media richness used and the acquired awareness levels of the recipients. The conclusion was that hypermedia, or online media, with interactive and adaptable forms of communication are the most effective for SAT. Similarly to the results of Puhakainen and Siponen [2010], it was emphasised that program should be continuous, to ensure that awareness is adequately maintained.

Observe success factors In the 2015 issue of the "Gartner Magic Quadrant for Security Awareness Computer-Based Training", an annual market evaluation of existing SAT program vendors, Walls [2015] summarised the following attributes as *strengths* for SAT programs:

- Continual and flexible analysis and reporting of user performance
- Flexible and customizable curriculum
- Interactive exercises
- Completeness and richness in terms of content
- Content optimized for variable device sizes
- High-frequency, short duration packaging
- Support for audience segmentation
- Support for multiple languages (not considered in this thesis)

2.1.3 Official Guidelines

There are several guidelines available, published by official organisations, that describe how to design an appropriate security awareness and training program. Two of the most common and comprehensive guides are described in summary here, with a focus on the attributes that are relevant for this thesis.

Special Publication 800-50: Building an Information Technology Security Awareness and Training Program

The U.S. National Institute of Standards and Technology (NIST) released in 2003 an extensive guide to aid the development and implementation of SAT programs [NIST, 2003]. Even though it is more than 10 years old, it still contains some valid pointers. The process is divided into three major steps: (1) designing and planning the program, (2) developing the material, and (3) implementing the program. In terms of planning, it is important to establish the program goals and intermediate objectives; what it is supposed to achieve. Then it is necessary to conduct a needs assessment to identify the current awareness and knowledge state of the employees. This will determine the required program effort and complexity of the material that is going to be developed.

Regarding the program content, it is emphasised that the material must be created relative to the organisation in which it will be deployed, with respect to culture and IT architecture. It is also emphasised that training material should be tailored to the learners roles and responsibilities. It is important that all personnel have a fundamental grasp (i.e. awareness) of security and potential threats and vulnerabilities. Building on that, employees should receive adequate training that allow them to work securely in their specific roles, according to their responsibilities and access levels. Before deploying the program, one must decide on the method of delivery, i.e. how the employees will engage in the program. It is suggested that the chosen method is easy to use, scalable, accountable and well tested. Lastly, NIST [2003] includes some "Program Success Indicators" that constitute attributes of successful program implementations; some of them are:

- Ensure support for broad program distribution.
- Use metrics to measure if the awareness and skill levels are increasing.
- Recognise employee security contributions (e.g., awards, contests).
- Management should strive to appear as advocates for good security behaviour throughout the company.

The New Users' Guide: How to Raise Information Security Awareness

The European Union Agency for Network and Information Security (ENISA) released in 2010 a similar document [ENISA, 2010]. The overall structure of the guide is much the same, and in some areas NIST [2003] is in fact used as reference. It also appears that this guide has a strong focus on how to obtain necessary program funding from senior management (which is not considered in this thesis). Nevertheless, the guide provides an apt list of "Obstacles to success". This list contains some useful pointers as to what should be given extra focus during the program planning and implementation phases; some of them are:

- One size fits all: It is important to adequately segment the target audience in order to deliver the right messages to the right people. Otherwise, it may not make the intended impression on the recipients.
- Too much information: Over-educating can often lead to the employees having a negative impression of the program.
- Lack of organisation: Consistency in terms of theme, style and delivery is important in order to build an identity for the program that the audience can get familiar with.
- Failure to follow up: It is important to actively keep the program prominent and fresh throughout the program lifetime.
- No explanation of why: In order to achieve the desired behaviour change, it is essential to clarify the reasons that support the policies.

2.2 Gamification

Building on the challenges, recommendations and best practices associated with security awareness and training, it is time to explore how gamification can complement this. As mentioned in the introductory chapter, gamification is the use of game design elements in non-game contexts [Deterding and Dixon, 2011]—a large variation of contexts. However, the focus in this thesis is a combination of *developing skills*, and *changing behaviour* among a target audience that is the *employees*.

2.2.1 Motivation

Motivation is at the core of gamification. Werbach and Hunter [2012] explain that the use of gamification typically consists in creating a new environment around an existing activity by introducing elements that will increase the motivation in doing that activity. Zichermann [2011] says that in order to create an engaging and meaningful system, it is important to determine how the system can "move the users along a path of mastery in their lives".

Self-Determination Theory

Ryan and Deci [2000] defined three distinct types of motivations for doing an activity: amotivation, extrinsic, and intrinsic. The model is called the Self-Determination Theory (SDT). It is presented as a continuum: amotivation is *nonself-determined*, which simply means that there is no motivation whatsoever for doing the activity, and people might do the activity simply without intent—or not do it at all. On the other side of the scale, intrinsic motivation apply to actions that are fully *self-determined*, i.e. actions are motivated purely by own will; e.g. fun or satisfaction. Between amotivation and intrinsic motivation, there is the extrinsic motivation, which is the type of motivation that comes from the outside. This is further divided into four different regulation classes:

- **External regulation** is often linked to actions that are motivated by rules and policies, and typically conforms to compliance.
- **Introjected regulation** concern actions that are done because the outcome is worth something to others.
- **Identified regulation** often applies to actions that one would consider beneficial to do, in the sense that the outcome might benefit the self (in the short or long run).
- **Integrated regulation** applies to activities that are almost self-determined. That is, the activity is congruent to a person's self evaluations and beliefs on personal needs. However, it is not considered as directly pleasurable.

Subsequently, Ryan and Deci [2000] further explained that there are three factors, or needs, that must be present for an activity to be intrinsically self-determined: competence, autonomy, and relatedness. Competence is related to the feeling of mastery; the impression of ability and triumph. Autonomy is much like free will, the feeling of being in control of an action; that it is not influenced by others. Relatedness is the feeling of meaning or purpose; that the action is connected to something greater than oneself. Figure 2.1 illustrates how the SDT continuum is arranged.

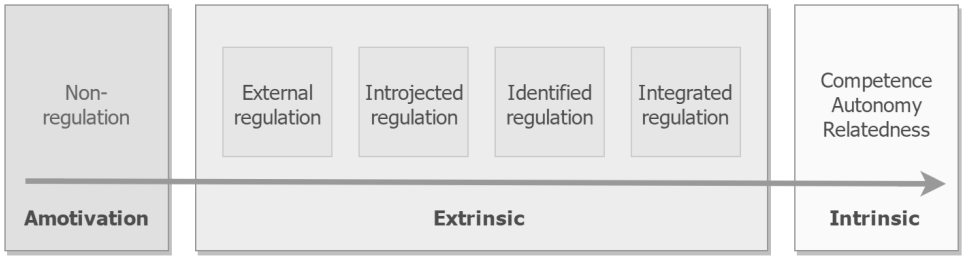


Figure 2.1: The Self-Determination Theory Continuum. The motive for performing an action is more self-determined the closer it gets to the intrinsic quadrant.

2.2.2 A Common Gamification Example

Gamification is a concept that is used extensively in marketing campaigns and customer loyalty programs. An example that is repeatedly mentioned in the literature is the Nike+ program to which owners of Nike running shoes can enrol and track their actual running progression [Nike, 2016]. The application will reward frequent runners with virtual prizes that they can share with their friends and fellow runners. This particular solution accomplishes something that is paramount to gamification, namely finding the crossing between the business' and the customer's goals: Nike wants to encourage people to purchase and use their products—and the customers (mostly) want to run and stay healthy [Burke, 2014]. Nike+ *motivates* people to do engage in an activity that they know they *should* do, but often do not *want* to do, which is typical example of the integrated regulations.

2.2.3 Developing a Gamified Solution

The gamification design framework that is used as main reference in this thesis is the scheme presented in the book "Gamify" by Brian Burke. Burke [2014] says the task of developing a gamified solution is first and foremost an exercise in constructing and shaping an experience. The experience design process consists in identifying what motivates the employees, what their goals are, and construct a path that will help them get there. Burke [2014] presents a seven-step iterative procedure for creating a gamified solution.

1. Define business outcomes and success metrics.
2. Determine the target audience.
3. Identify the player goals.
4. Define the engagement model.
5. Decide the play space and journey.
6. Establish the game economy.
7. Play test and iterate.

The first two steps are not considered in this thesis, as they are fundamentally connected to the individual organisations that are going to use the solution. Defining the desired business outcomes and success metrics involves answering the questions "why is the solution needed?", and "what does success look like?" Next, one must identify and map the target audience. This is typically a process of getting to know and understand the actual users of the application—the employees; what triggers their engagement? The remaining steps are explained in more detail in the following sub-sections.

Shared goals

Step three is to figure out what the employees' goals are. *Why should they want to get educated in the field of security?* The idea here is to try to identify objectives that are common for both the company and the employees, in order to create a focus that is not merely influenced by managerial decisions. Finding these shared goals will be integral to the success of the gamified solution [Burke, 2014]. As in the Nike+ example, Nike found a way to promote their products by inspiring customers to do something that would also benefit themselves; achieve an internal goal (i.e. being healthy).

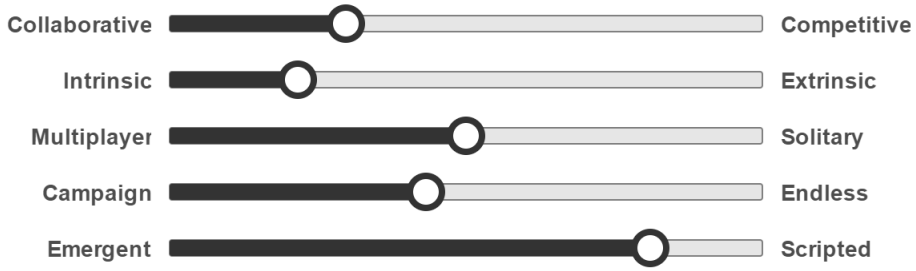


Figure 2.2: The engagement model, determining how users interact with the solution. Reproduced with permission from Bibliomotion, Inc. (Gamify: How Gamification Motivates People to Do Extraordinary Things by Brian Burke, Bibliomotion, 2014).

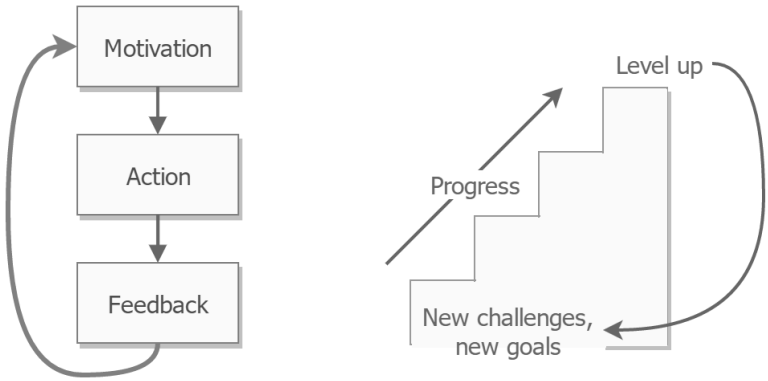
Engagement model

The *engagement model* defines how the users will interact with the solution [Burke, 2014]. This includes how the application is structured, and how the player is positioned against the tasks and content, and the other players. Figure 2.2 illustrates how different engagement aspects need to be balanced in order to create the appropriate game environment. For example, one must decide to how the users will interact with each other, that is, competitively or collaboratively. One must also determine to which degree intrinsic motivation is achievable, and how extrinsic rewards (points, achievement, or physical prizes) can be used to additionally boost motivation. Zichermann [2011] says a solution should rely on both extrinsic and intrinsic rewards to drive short and long-term behaviour, and in fact, if used correctly, extrinsic motivators can be adopted as intrinsic motivators if players find joy or pleasure in trying to achieve them. Burke [2014] further explains that it is important to determine whether the *journey* to the end goal is going to be scripted—i.e., all the players go the same path—or if the players will have some freedom to explore and shape their own route to the end goal.

Play space and journey

The play space is essentially where the solution unfolds, whether it be in a virtual environment that comprises the game, and/or activities that exist in the real world [Burke, 2014]. For example, if a gamified solution was set up to motivate employees to report real phishing attacks, then this would involve both a virtual and real world environment. As Burke [2014] further describes, the journey details how the user is guided through the game and towards the goals. This includes how challenges should correspond to the skill level of the player at each point in the game, in order to maintain engagement from beginning to the end. The journey also says something about how and when the players should receive feedback for their efforts in the game—e.g., when to receive points, rewards, or level advancements.

The journey is also mentioned by Werbach and Hunter [2012], illustrated by two *activity loops*. The first loop is called the engagement loop, depicted in Figure 2.3a. It begins with a player's motivation to perform an action, which is then rewarded, or recognised, through some form of feedback. The feedback will again work as motivation to proceed to new actions. The second loop is the progression loop (Figure 2.3b), which basically defines the levelling process in the game. The user completes some tasks that earns progression towards some goal. When the goal is reached, the user is presented with new tasks that will focus on the next goal, and so on—until the ultimate goal is reached. The loop is a way to keep segment the journey into smaller pieces, such that the player can concentrate on smaller achievable objectives rather than only playing for a final goal that may seem unobtainable.



(a) The engagement loop **(b)** The progression loop

Figure 2.3: The activity loops, illustrating how to maintain the player's enthusiasm to continue playing.

Game economy

The next to last step is to establish the *game economy*, which in some ways represent the most hands-on motivational factors. This is a crucial step that will determine the rewards, feelings, and sentiment that the users will receive and experience when interacting with the solution. Figure 2.4 shows four different categories of such motivational factors derived from games. When designing a gamified solution, it is important to consider all four categories, however factors from *self-esteem* and *social capital* are thought to be the most suitable and relevant [Burke, 2014]. Similarly, Chou [2015] describes eight "core drives" that can affect human engagement: meaning, accomplishment, empowerment/feedback, social influence/pressure, unpredictability/curiosity, ownership, impatience, and loss avoidance. The functionality and features of a solution should attempt to target on one or more of those drives. Moreover, Chou [2015] expresses that elements can advantageously be altered or modified to target other drives as the player progresses in the solution's journey.

Final step

As with any new application, the last and final step is to test, evaluate—and iterate. It is important to take note of what worked, and what needs improvement and then implement this through a new iteration. For each repetition, the application will become better and more tailored towards the environment it is supposed to be used [Burke, 2014].

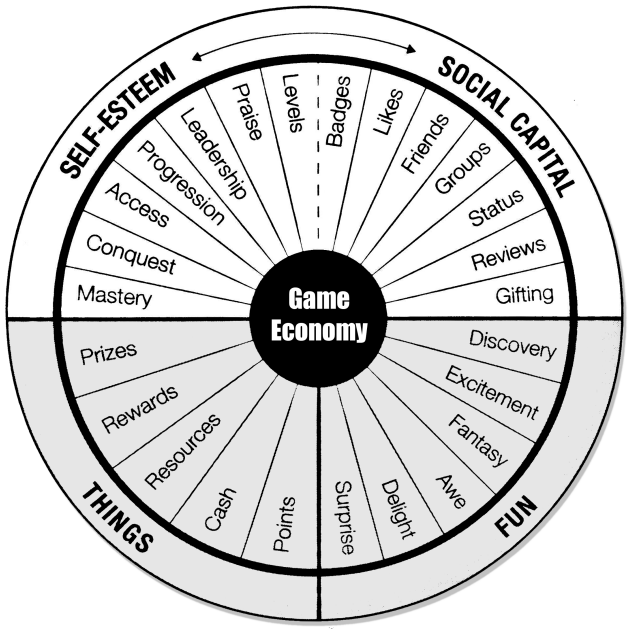


Figure 2.4: The game economy, factors that can motivate people to play. Reproduced with permission from Bibliomotion, Inc. (Gamify: How Gamification Motivates People to Do Extraordinary Things by Brian Burke, Bibliomotion, 2014).

2.2.4 Does It Work?

In the recent years, many studies have tried to assess the effects of gamification. Hamari et al. [2014] conducted a review of 24 empirical studies to investigate if gamification actually works. The conclusion was that gamification has in fact shown positive effects in improving learning outcomes on multiple occasions. However, it was emphasised that the effects depend on the users and the context in which the technique has been applied. It was also noted that there are currently few high quality studies on the actual effects of gamification.

In 2012, Gartner said that 80% of all current gamified applications would fail to meet business objectives, primarily due to poor design [Burke, 2012]. It is not clear whether this prediction turned out to be true, however, in 2013 Gartner also placed gamification at the "peak of inflated expectations" in their "Hype Cycle for Emerging Technologies", and anticipated that it would enter "the trough of disillusionment" in 2014 [Burke, 2014]. Even so, it was still predicted by Gartner that by 2017, "50% of Global 1000[2] organisations will use gamification in learning and/or recruitment

[2]Global 1000: the world's thousand largest organisations in terms of revenue.

processes", emphasising that gamification does in fact have great potential. Burke [2014] says that many applications fail because of three principal reasons: (1) that the business outcomes have not been clearly defined, (2) that the solution only focuses on the organisational goals, rather than the goals of the players, or (3) that the solution only engages players on a transactional level (i.e. extrinsically), and not on an emotional level.

The latter argument is further illustrated as Werbach and Hunter [2012] warn of falling into the trap of merely using some of the most basic traits; the points, badges and leaderboards—also called the "PBL-triad" . While these elements are some of the most common and fundamental elements of gamification, they are by far not the only ones; there are many other, perhaps even more important, ways of creating motivation, such as in the steps described in the previous section. Several game designers have emerged as critics of gamification: Robertson [2010] argue that gamification is falsely claiming to be related to game design, because many implementations of gamification often focus on extrinsic rewards—such as the "PBLs". Robertson [2010] explained that these are not the among the elements that make games intrinsically motivating. Bartle [2011] added that points and achievements are for the most part only valuable if the community recognises them as valuable. If you have a lot of points, but nobody cares, you will not get that mastery feeling. Deterding [2011] uses the words "meaningful play" to illustrate the importance of intrinsic motivation (competence, autonomy, and relatedness from SDT) as part of gamification. [Werbach and Hunter, 2012] adds that successful gamified solutions should employ many different motivators in order to reach out to as many players as possible—because people are motivated by different things.

2.3 Previous Studies on Gamified SAT

Unsurprisingly, the idea of using gamification in SAT is not novel for this thesis. However, most existing studies seem to employ a different definition and practice of gamification than the one used here. As Werbach and Hunter [2012] emphasise, gamification is not the same as serious games; actual games (virtual worlds), or computer simulations of real world scenarios, created for educational purposes. Consequently, studies that merely consider the use of actual video games in SAT programs (e.g. CyberCIEGE by Cone et al. [2007]) are not considered here. There are however a couple of moderately related studies that are discussed here.

Thornton and Francia [2014]

This study provides a good summary of gamification elements and design strategies, however, it appears that the main focus is to create actual games. Multiple games are presented in the study, though the results refer to a "tower defence game" aimed at teaching students about password strengths. It is not clear which aspects of gamification that were used in the game. The game was played by approximately 180 students.

The results claim that the game was consistently effective in increasing awareness among the students. There are however some significant limitations to this study: firstly, the results were collected through a self-reporting survey, where the participants rated statements on a scale. Example statements were: "I am more aware about what makes a strong password", and "I am more aware of the importance of not re-using passwords". It is not evident that these results prove that gamification is in fact effective for SAT. Secondly, it was not described how gamification was used in the solution. Judging from screenshots included in the report, it appeared that the use of actual gamification techniques was minimal.

Baxter et al. [2015]

The gamified solution in this study utilises elements such as a story, goals for the employee, feedback and progress. The authors acknowledge however that the solution lacks "other gamification techniques such as competition based on points and leaderboards, achievement badges or levels, or virtual currencies". The game follows a fictional investigation of a breach of security which may have compromised an international bank's customer data.

The study evaluated the effectiveness the solution in two different experiments. First, it was assessed how the solution rated against (1) no training, to determine if gamification would be able to educate at all, and (2) training without gamification, to see if it was better than traditional training. This experiment was conducted with

university students; 33 students used the gamified solution, 45 students received no training, and 38 students completed the traditional non-gamified training. The experiment lasted for 30 minutes. All students completed a knowledge quiz after the training. Results showed that the gamified training is better than no training, but actually less effective than traditional training. The respondents of the traditional training outperformed the gamification test group by 3.1%.

In the second experiment, a much larger population was used to assess the difference between gamified training and no training. The participants were employees at a bank. 531 employees completed the training with a following knowledge test, while 325 only completed the test. The results showed that the gamified training did *not* improve knowledge acquisition. In both experiments, the users of the gamified solution did however rate the training as more enjoyable, more fun, and less boring than the ones using the traditional training.

The authors identify two main limitations for the study. Firstly, as already mentioned, the gamified solution was missing some of the core elements of gamification, which could have been decisive for the overall results. Secondly, the training was short in duration, and only a one-time effort—and thus not able to assess the long-term effects. The study differs from this thesis primarily in the way that gamification is used, and the research design; whereas this thesis takes a more qualitative approach, though with a considerably smaller population.

Chapter 3
A Gamified Security Awareness and Training Program

The first part of this chapter presents the main concept, or idea, that is the basis for this study, which is meant to demonstrate one possible approach to the use of gamification in security awareness and training. The concept is based on the literature that was reviewed in the previous chapter, and some initial ideas that were devised during the framing of the thesis problem description. The concept also finds inspiration in a few existing gamified systems, which are described here. Additionally, some similar commercial products are briefly mentioned. The second part of the chapter introduces the prototype that has been developed during this study.

3.1 The Concept

In summary, the main idea is to have a long-term SAT program where the main component is a gamified learning application. The application contains security awareness material and training exercises wrapped in a gamified experience that aim to create engagement and motivation around the learning process. The general circumstances around the application are the following:

- The employee controls when and where the training takes place by accessing the learning application through a web browser or an associated mobile application.
- There should be a large selection of tasks and exercises divided into different security categories. There should also be different types of tasks to attain diversity in the learning environment. The content should aslo be regularly updated and extended.
- The exercises should be concise and compact. Each task or exercise should take only about five minutes to complete.
- The employee is free to complete any exercise they want, in which ever order they want. This gives a certain amount of autonomy and thus a more emergent engagement model in that employees do not have to follow a strict path.

However, some restrictions must apply to ensure that the employees receive the required type and amount of training.

Remark It should be clarified that there is a difference between the SAT *program* and the gamified application. The program itself is a more administrative instrument that may contain other awareness material such as hallway posters, intranet newsletters, or other activities that an organisation may find appropriate. The application is the component that constitutes the main use of gamification in the program. The prototype that is presented in the subsequent part of this chapter is an example of such an application.

3.1.1 Delivery model

The gamified application can typically be offered as a Software as a Service (SaaS) solution, where the software and content is provided and maintained by a third party provider. This way, companies will not have to cater their own hosting, allowing the solution to be more centralised—which will also ease the process of application updates. Furthermore, by fetching the content from a central source, it can be updated more frequently.

3.1.2 Inspiration

In the recent years, several gamified systems have emerged, and some of them has seen significant popularity. Consequently, some inspiration has been extracted from these systems.

Duolingo

Developed by Luis von Ahn and Severin Hacker, Duolingo [2016] is a free software application for language education. It employs extensive use gamification—one of the slogans being "Gamification poured into every lesson". Duolingo has been of inspiration in two ways: first is the use of short and compact lessons. A Duolingo lesson is typically completed in only a few minutes. This allows for a user to complete exercises during small breaks that naturally occur during a day, for example while waiting on the bus, while riding the bus, or while waiting for the pasta to cook. Thus, an employee will not have to schedule the training and use valuable work hours to complete a long and tiresome course. The second feature of Duolingo that has been of inspiration is the one where your acquired skills decrease as time passes—i.e. you have to go back and repeat certain subjects if some amount of time has passed since you last touched on them. This particular element can serve as a useful technique to handle the repetition of training.

Khan Academy

Started by Sal Khan, Khan Academy [2016] is another gamified educational system that has seen huge success. This learning portal makes extensive use of gamification elements like points, badges and progression graphs to motivate users to watch educational videos and solve exercises. Consequently, Khan Academy is an inspiration in itself, in that it has successfully influenced huge amounts of people (42 million as of May 2016 [Khan Academy, 2016]) to engage in learning activities they perhaps otherwise would not.

QuizClash

QuizClash [2016] is a quiz application for mobile devices developed by FEO Media. The application allows people to challenge each other and compete in a wide variety of subjects. Once a challenge has been initiated, both players will receive a set of identical questions drawn from some pool. The players then answer the questions to their best effort, and the winner is the one who answered most questions correctly. It is a simple set-up, but can be very engaging. The use of this idea is illustrated in the prototype under the name "Challenge-a-colleague".

3.2 The Prototype

This section introduces the prototype application that was developed as part of this study. The prototype constitutes a limited representation of the concept explained in the previous section. There is only a selection of gamification elements present, but it functions as an example of what a gamified solution might contain. The elements are explained in accordance with the gamification design process that was presented in the previous chapter.

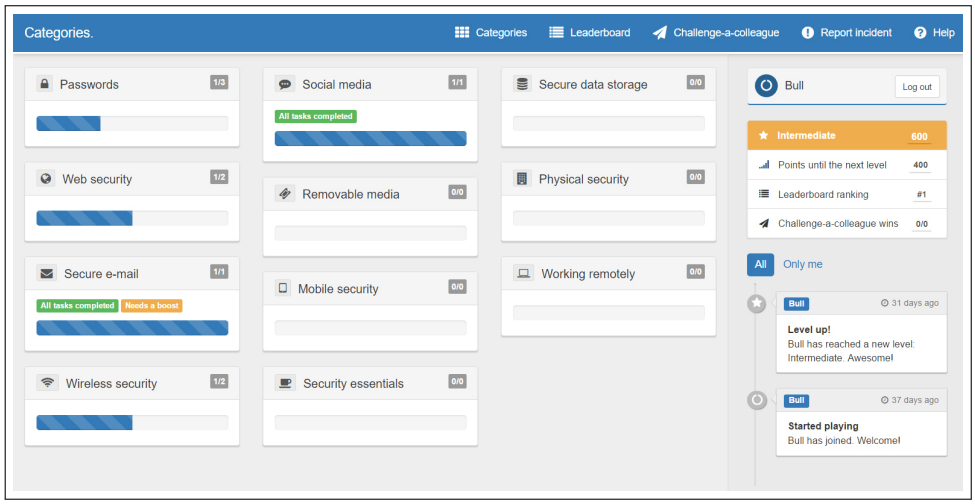


Figure 3.1: An overview of the prototype application interface.

3.2.1 User Interface

The full-screen user interface of the prototype is shown in Figure 3.1. In the following subsections, the interface is decomposed and the different components and application views and components are explained separately. The navigation bar at the top and the sidebar at the right side of the screen are static elements that are present for all views. The prototype relies mainly on single-player engagement model where players control their own progression independent from others.

Category view

The category view is shown in Figure 3.2. This is the first view that loads after the user logs in. Here, all the categories are displayed in separate boxes. The user can click any category to see the exercises comprised in the category. In the top right corner of each box is a statistic of how many tasks the user has completed in the category, of the total available amount. In the middle of the box is a progress bar giving a visual representation of the same statistic. If a user has completed all

the tasks in a category, a green label with the text "All tasks completed" is shown. Additionally, a yellow label can appear, saying "Needs a boost". This occurs if it is a long time since the user has completed exercises for a specific category. An example of this is shown in the "Secure e-mail" category in Figure 3.2. This may happen regardless of whether the user has completed all the exercises for that category or not. The idea for this feature was inspired by Duolingo [2016]. *This particular feature is however not functionally operative in the prototype, and is only present for illustration purposes.*

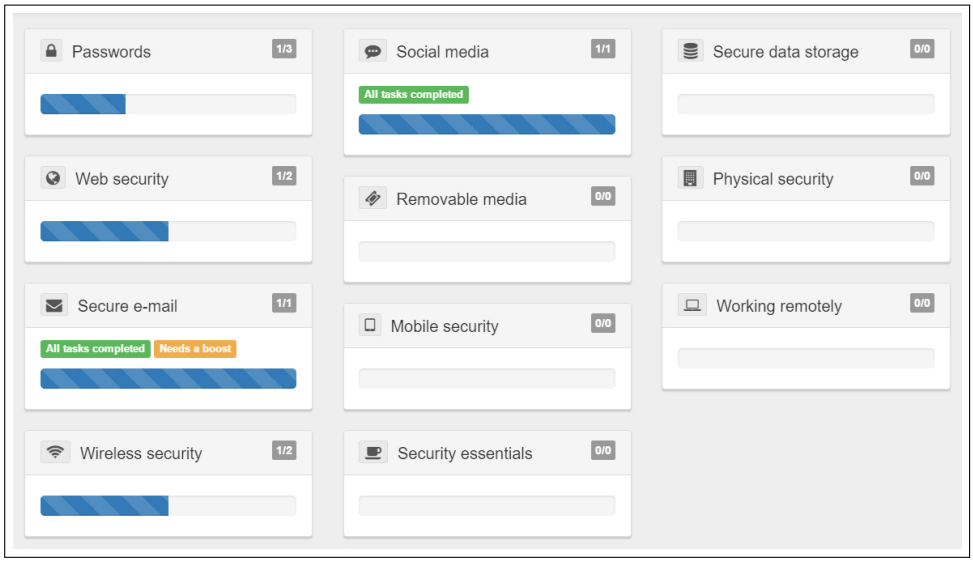


Figure 3.2: The category view. The categories shown here are the sample categories that were outlined for the prototype, however only five of them contains exercises.

Sidebar

The sidebar component is shown in Figure 3.3. This is a static part that is always displayed on the right side on the desktop and tablet versions. On smaller screens, the sidebar is located on the bottom of a view. The sidebar contains several meaningful elements. The top box shows the user avatar, alias and a button for logging out. The box below contains the user's current skill level and the points counter, followed by a hint on how many points the user needs in order to get to the next level. Next is the user's ranking on the global leaderboard, and the bottom row shows the user's current score in the colleague challenges (this feature is presented in a subsequent section). Points are awarded for completing various activity inside the application. If a user reaches some specific amount of points, the skill level will increase. The points and levels function both as rewards and as indicators of progression in the game economy. In a social context, it might also amount to a sense of status.

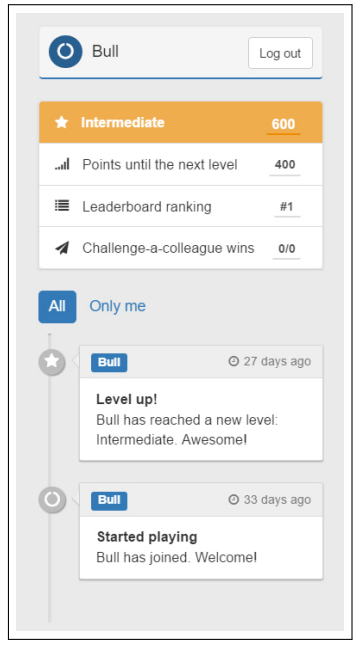


Figure 3.3: The sidebar.

The last constituent of the sidebar is an activity timeline that shows recent events in the application for all the users. This way, the users get real-time updates on the achievements of other users. Examples of events that can appear here are when a new player signs up, when a user reaches a new skill level, when a user gets a new achievement, or when a user completes all the tasks in a category. *Not all the events were implemented in the prototype.* This element is intended to spark competition between users, in the way that some might be motivated to work harder if they see that others are progressing. It is also a good way for users to track their own progression and achievements. Additionally, knowing that others see your achievements may increase self-esteem.

Task view

When a user clicks a category, the task view is displayed. Figure 3.4 shows the task view with three sample exercises from the password category. Each task is displayed in its own box. On the top of each box are two labels that describe the difficulty level of the exercise and what type of exercise it is. Then comes the title of the exercise, followed by three statistical items: first is the amount of points that is achievable for completing the task, followed by a count of how many people that already have completed the task. The second statistic is meant to have two functions: if the count is high, it means that someone else has spent time doing it, i.e. it has some value to

others, and because of that, it can appear more motivating to do it. Vice versa, if no one has completed the task before, it may give a sense of mastery to be the first one.

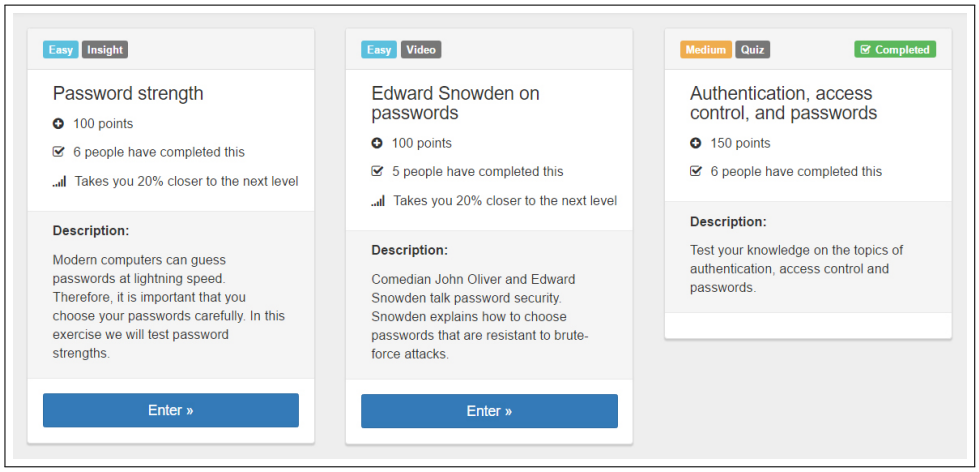


Figure 3.4: The task view, here showing the sample exercises in the password category, where one of the exercises has been completed.

The last statistic is a calculation on how many percent closer the user will be to the next level if they complete the task. If the task holds enough points to bump the user all the way to the next level, it will simply say "Takes you to the next level". This calculation is meant to turn the users' attention to the intermediary objectives, and show that the next level is "not that far away". The last item in the task box is a short description of the task and what the user can expect to learn. When a task is completed, a small green box is displayed to salute the user on the success, as shown in Figure 3.5. It was considered important to use positive messages in order to stimulate motivation for further use, according to the engagement loop (Figure 2.3a). A green label saying "Completed" will be shown in the top right corner of the task box.

Task types

Five different types of tasks were developed for the prototype, as a way to provide a diverse learning environment.

Lesson This is the more traditional form of exercise, where the user must read some text. However, it was ensured that the content was concise and divided into short paragraphs. The user has to check a box saying "Got it!" before moving on to the next paragraph. This task type can convey short chunks of information that will be necessary to solve other exercises.

Quiz The tasks of this type follow the typical structure of a quiz: a question and some answer options. The quizzes in the prototype contain around 10 questions. There is also a "true or false" variant, as shown in Figure 3.5. Users are able to go back and correct the answers they got wrong, as to let everyone earn the points. A side effect of this is that it removes the drive of loss aversion (Section 2.2.3).

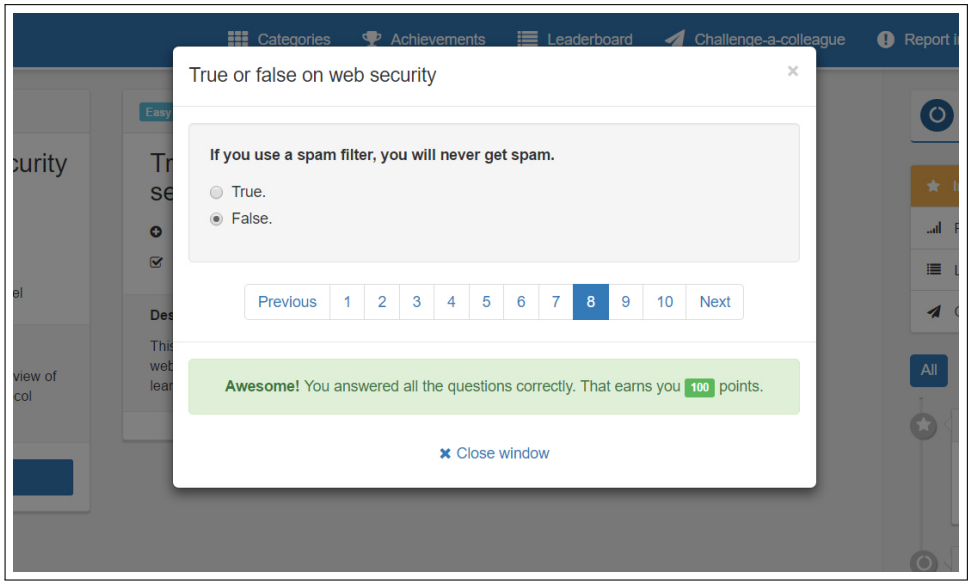


Figure 3.5: A example of the feedback the player sees when completing a task, emphasising positive reinforcement.

Article Tasks of this type present the player with a news article that reports a "real world" security breach. The chosen articles also include suggestions for how to avoid such breaches. Purposely, this task type was created to let users see that security breaches are real, and provide an insight to how attacks unfold. It is also considered an advantage that suggestions for good security behaviour come from other sources than just the company management. The articles broaden the play space by bringing the players out of the game environment. When the players return to the application after reading the article, they have to answer a control question (with answer options) taken from the "how to avoid attacks" section of the article.

Insight These exercises are intended to give players a broader and more comprehensive insight into why security is important. The exercises should have high levels of interactiveness and visualisation. However, in the prototype, there is only one exercise of this type; one about password strengths (see Figure 3.4). This exercise let players input several passwords, and get a calculation of how long it would take a normal computer to guess the password. The calculations were based on formulas by

NIST [2013]. The purpose of the exercise was to let the players discover the patterns of strong passwords on their own. Points were awarded after 10 passwords had been tested.

Video Lastly, this task type simply includes a short video clip that addresses or explains some security related matter. The two clips used in the prototype are about password strength and web security, respectively. The clips were retrieved from YouTube[1].

Leaderboard

From the navigation bar, the players can go to the leaderboard view to see who has the highest scores. Figure 3.6 shows a leaderboard with three sample users. Players can choose to filter the board to show only users from their department, or users that they have added as their friends (*functionality for joining a department or adding friends was not implemented; it is just for illustration purposes*). This way the users can individually choose which level of competition they wish to engage in; if they want to compete against all users, or just a selection of colleagues—or if they are not concerned about competition, they do not have to pay attention to it at all. However, for those who feel engaged by it, it will contribute to a more competitive engagement model. For the players who achieve a high ranking, the leaderboard can provide feelings of conquest and mastery. In terms of social capital, it can give a sense of status.

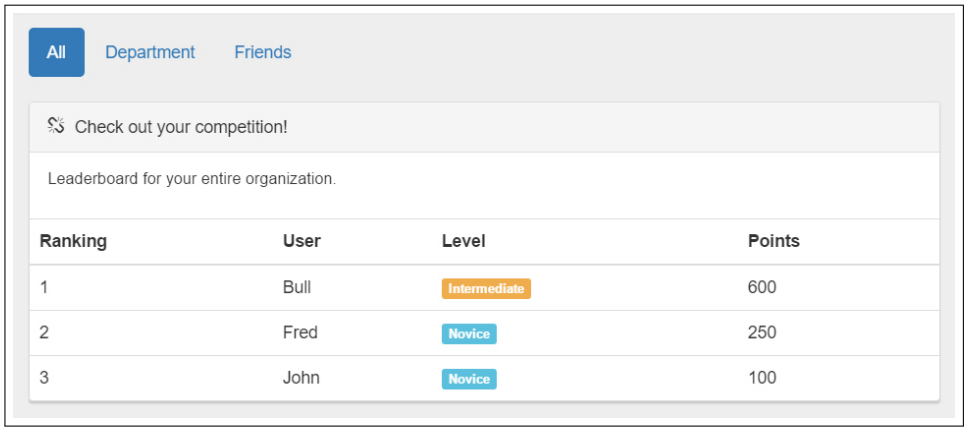


Figure 3.6: The leaderboard, here showing three sample users. The buttons to filter the board are located on the top.

[1] YouTube; `https://www.youtube.com` (2016 YouTube, LLC)

Challenge-a-colleague

An idea for the prototype was to have a feature similar to the quiz application Quiz-Clash [2016], where players could challenge each other to a quiz battle. Unfortunately, due to time constraints, this feature was not implemented. However, for illustration purposes, there is a button in the navigation bar that opens a dialogue box, as shown in Figure 3.7. The user would input the alias of the colleague they wish to challenge and select a category to compete in. A quiz should then be generated with questions randomly chosen from the category. The player who answers the most questions correctly will receive 100 points from the other player. This feature was created for the competitive player with the following ideas in mind:

- It could make people do more training.
- It could make people repeat subjects more frequently, as questions would likely be replayed.
- It could help bring players into the application more frequently, which could result in further activity in other parts of the solution.
- It could collectively engage more people: if someone gets hooked, they could engage other employees to use the application.

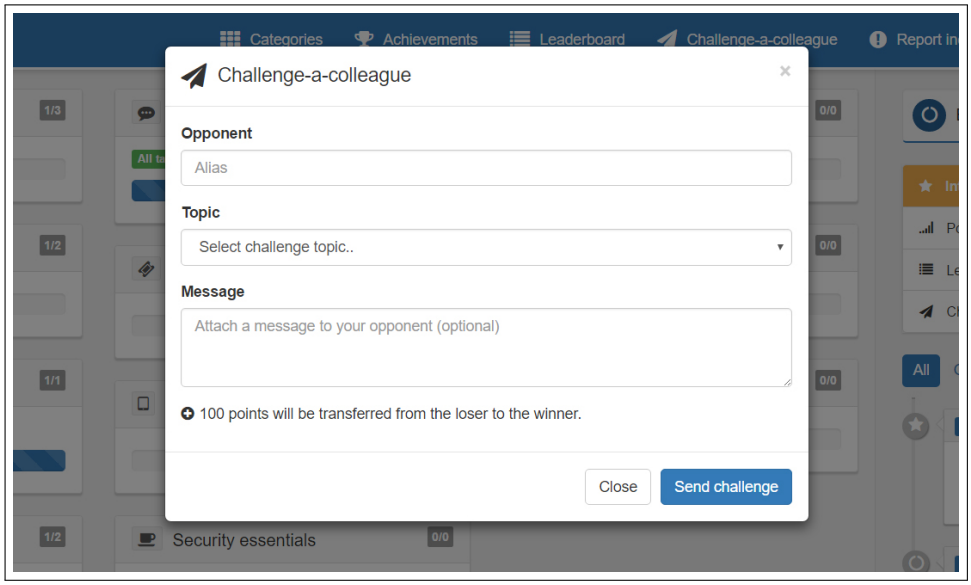


Figure 3.7: The thought "Challenge-a-colleague" interface from where players could challenge other colleagues on security related topics.

Report incident

Similar to the previous one, another idea that did not get implemented, is a feature where users can create reports of security incidents that they have observed. This could for example be phishing email they have received, data leaks they have discovered, software vulnerabilities they have found, or fake hotspots they have detected. The reports could be evaluated—or investigated—by a security manager. If the report turns out ot be valid, the user should receive a sizeable amount of points for their efforts; here set to 200. This particular functionality extends the play space to include actual security events from outside of the application—or game. The idea behind this constituent is to let users actively engage in the process of identification and prevention of security incidents. At the same time, it builds a database of incidents that can be available to employees and also work as material for future exercises. User reports can also help to contain security breaches, minimise damages, and perhaps shorten response times. An example interface is depicted in Figure 3.8.

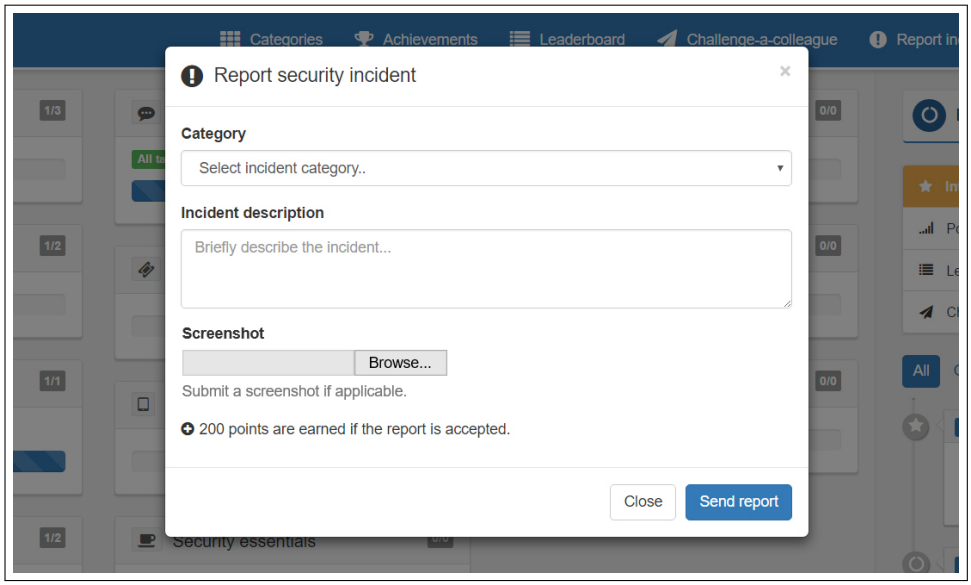


Figure 3.8: The thought "report incident" interface from where users can report real life security events.

3.2.2 Technology

The prototype utilises an untraditional, yet simple infrastructure, focusing on easy deployment and database management. Figure 3.9 gives a high level illustration the infrastructure. The application is accessed through a web browser.

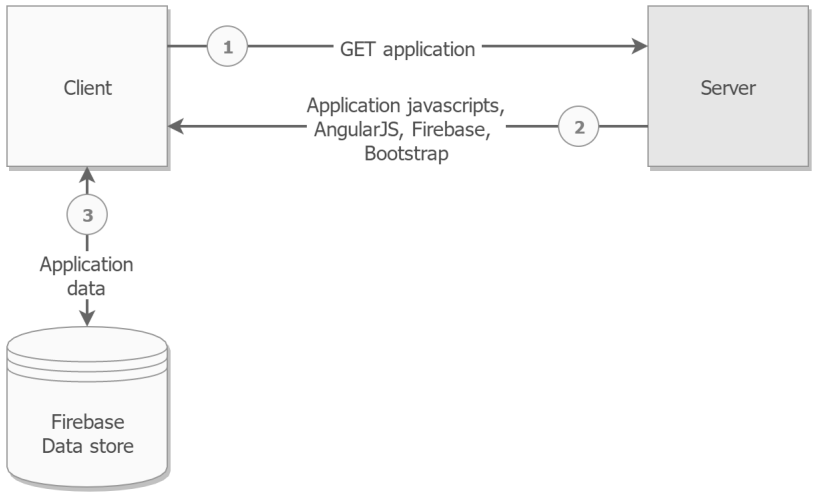


Figure 3.9: High-level overview of the prototype application infrastructure.

Database

The database management system selected for the prototype is Firebase [2016]. This is a NoSQL[2] database that stores data as JavaScript objects. Firebase also comes with a full-scale authentication Application Programming Interface (API) that handles user sessions seamlessly straight out of the box. Additionally, Firebase lets client side JavaScript query the database, which means that there was practically no server code needed in order to create a fully functioning prototype. The database was hosted online at Firebase[3].

Client

The client side was developed in JavaScript using the AngularJS [2016] framework, which connects flawlessly with Firebase—as they are both Google products. The entire application logic, e.g. user registration and assignment of points and levels, was implemented on the client side[4]. Firebase also includes a feature called "three-way data-binding" that enables real-time updates, such that leaderboard and activity timeline will update on all clients instantaneously upon change. Additionally, the Bootstrap [2016] grid system is used to make the application responsive to various screen sizes, such that it scales well on smaller screens, such as smartphones.

[2]A NoSQL database handles storage and retrieval of data using other mechanisms than the tabular relations used in relational databases [Wikipedia, 2016a].

[3]Hosting at `https://firebase.google.com`

[4]This is not a good practice for real systems, as users can in practice assign points to themselves, however it worked well as a speedy solution for the prototype.

Server

As mentioned, the server instance required minimal coding. The only purpose of the server instance is to provide the application JavaScripts (including AngularJS, Bootstrap, and Firebase) to the client upon request. This functionality was implemented in Node.js [2016] and run locally.

3.3 Similar Products

After some browsing on the web, it was discovered that there are in fact some commercial products available that resemble the idea proposed in this thesis.

Awarity

Awarity [2015] is a mobile application developed by Awarity Training Solutions in Austria. The idea presented on their website seems quite similar to the one proposed in this thesis: "Aspects of Gamification will be used to motivate your employees over a long term period." They also claim to be the the first gamified training platform for security awareness. It appears that the application is still in a demo phase.

Apozy

Apozy [2015] is a U.S. based company that develops a gamified security awareness product with a focus on generating metrics to facilitate risk management for human information security in enterprises. Judging from the (sparse) information available on their website, the impression is that it might be quite similar to the concept that is proposed in this thesis, and also the one of Awarity. The product is not yet released.

BeOne Ubiq

BeOne [2016] is one of the larger commercial SAT program vendors. It has a mobile application called BeOne Ubiq that allows employees to do training "on demand", which is in fact one of the more prominent elements of the concept considered in this thesis. It seems however that this application does not incorporate gamification.

Chapter 4
Research Method

This chapter describes the research approach. The methods used to collect qualitative data are explained in detail. The companies and people involved in the study are briefly described. Conclusively, the data analysis method is discussed.

4.1 Research Design Strategy

The chosen research design is of the *flexible* type [Robson, 2011]. This includes qualitative methods for data collection, where results are given in words rather than numerical values. As Robson [2011] describes, the flexible design is not an "off-the-shelf" research approach. Even though there are some established traditions for this type of research, sometimes the design needs to be constructed according to the research questions in order to achieve the desired results. A step-wise overview of the research approach for this study is shown in Figure 4.1. There are two main reasons as to why the flexible research design strategy was chosen for this thesis:

- **Time**: The implementation, full-scale deployment, and testing of a software solution; with acceptable results, would require more time than what is allocated for this thesis.
- **Nature of the study**: The desired output of this thesis is to gain insight to if, and possibly how, gamification can provide a more engaging learning environment for security and thus give added motivation for practising good security behaviour. It makes sense to discuss this actual matter with the end users. Moreover, as was described in Chapter 2, the gamification design process emphasises the need for communication with end users to be able to implement an effective gamified solution.

Correspondingly, the research approach resembles a small scale, single iteration instance of the Design Science Research Process (DSRP), as it is described by Peffers et al. [2006] (Table 4.1).

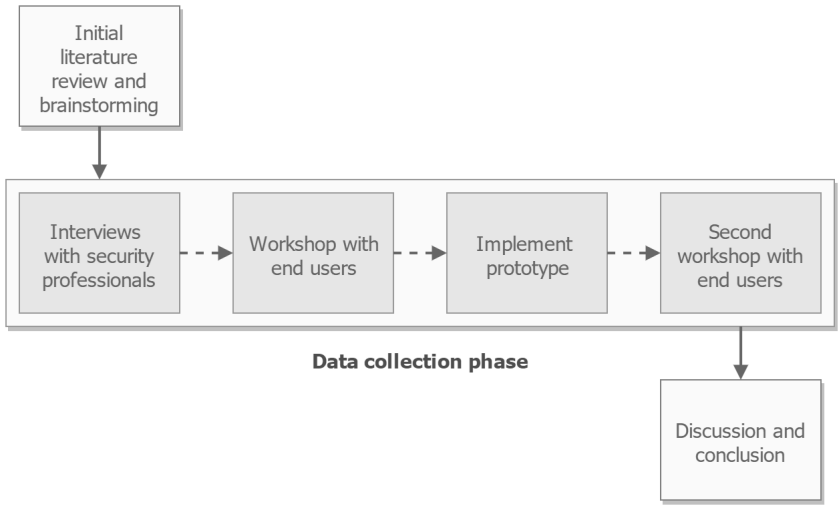


Figure 4.1: The steps in which the research was conducted. Interviews and workshops were run concurrently at the two participating companies.

Table 4.1: The Design Science Research Process (DSRP) by Peffers et al. [2006].

1	Problem identification, motivation	Define the specific research problem and justify the importance and value of a solution.
2	Objectives of a solution	Deduce the objectives of a solution from the defined problem. Identify how a new solution can improve on existing ones.
3	Design and development	Create the artefactual solution: determine the desired functionality and architecture, and create the actual artefact.
4	Demonstration	Find suitable context and demonstrate the artefact's efficacy to solve the defined problem. This could involve its use in experimentation, simulation or a case study.
5	Evaluation	Measure how well the artefact supports a solution to the problem. Compare observed results with the objectives. Iterate back to step 3 to improve the artefact, or leave further improvement to subsequent projects.
6	Communication	Scholarly or professional publications. Communicate the problem and its importance, the artefact and its utility, the rigour of its design, and the demonstrated effectiveness.

4.2 Data Collection Context and Methods

The data for the study were collected through interviews and workshops with representatives from two Norwegian companies, A and B. This permitted a wider range of results, and comparability between two different industry sectors. Both companies are knowledge-based businesses, in the sense that they do not manufacture or sell physical products. However, the two companies are not direct competitors. Their headquarters are located in two different Norwegian cities.

The interviewees A total of five individual interviews were conducted, two at company A and three at company B. The interviewees were employees with several years of experience working with security. Most of them also have direct experience with security awareness and training programs.

The workshop groups The workshop participants were mostly employees that did not work directly with security, but that had experience with other existing security awareness and training solutions. Each group consisted of five participants. At company A, the group consisted of two representatives from the human resources department, one quality and security leader, and two knowledge workers; one of which has security as their main area. At company B, all the participants were from the human resources department. It was considered important that the same group participated in both workshops, as they were widely connected.

4.2.1 Interviews

The main focus for the interviews were research questions 1 and 3 (from Table 1.1). An interview outline (Appendix A) was issued to the interviewees a few days prior to the scheduled interview, to let the interviewees get a feel for the topics that were going to be discussed. However, the interviews were conducted in a *semi-structured* manner [Robson, 2011]. The questions asked were open-ended, and the interviewees were encouraged to elaborate and use examples to illustrate their answers. Consequently, some answers varied in both content and length. The answers were recorded with pen and paper only. All interviews lasted approximately 45 minutes to 1 hour. The results are given in Section 5.1, compiled under three different topics, as given in Table 4.2.

4.2.2 Workshop 1

The main focus for the first workshop were research questions 1 and 2. Before the workshops started, a single-page document (Appendix B), explaining the plan for the data collection, was prepared and sent to the participants. In the first workshop, the discussions revolved mainly around three selected topics, given in Table 4.3. A

Table 4.2: Topics that were discussed in the interviews.

Topic	Motive
Security awareness and training	Determine challenges related to security policy compliance, and identify elements in current training methods that have proven successful.
Gamification	Discuss why good security behaviour should be a goal for employees, and identify factors that support the use of gamification in security training programs.
Long-term, continuous training	Evaluate whether a gamified, long-term continuous training program is in fact feasible and expedient.

set of slides, including some exercises, were prepared in order to guide the discussion through the topics. The session was opened with a general discussion on information security to get the correct mindset and start the ball rolling. In order to lighten the mood, a humorous video about security awareness was shown. The discussions then continued on the subjects of existing solutions, and their strengths and weaknesses. After a short break, there was a brief introduction to gamification. Then there was an exercise where a short advert for the Nike+ program (mentioned in Section 2.2.2) was shown, and the interviewees were asked to take note of all the gamification elements they could identify. The findings were then discussed in plenary. The rest of the session was dedicated to discussions on gamification; shared goals and game economy, following the model of Burke [2014]. The results were recorded with pen and paper and sound recording. The session lasted for two hours (limited). The results are given in Section 5.2.

Table 4.3: Topics that were discussed in the first workshop.

Topic	Motive
Existing solutions	Identity factors in existing SAT solutions that should be continued in a new solution, and also factors that should be improved.
Shared goals	Identify overlaps between the desired business outcomes and the users' motivations for good security behaviour. Why is it important to learn about security?
Gamification motivators	Identify which motivational factors that users consider the most important, based on the game economy introduced in Chapter 2.

4.2.3 Workshop 2

After the first workshop, the results were analysed and integrated with the results from the interviews and the literature study. Subsequently, the prototype application was implemented. The main focus for the second workshop was research question 3—in the perspective of the employees. The approach was to let the participants test the prototype in order to get a hands-on impression of what a gamified security training solution might look like. The data were recorded with pen and paper.

Test set-up

Since the prototype only had limited functionality, and the fact that workshop would not allow the testing of the long-term effects of the program, the participants were given a thorough walkthrough of the concept as given in Chapter 3 before the testing commenced. The participants were asked to *envision* the full extent of the concept and the concept while testing. The participants were given directions on how to connect to the application and create an account. After all participants had registered a user, a brief introduction was given to the user interface, however it was intended that the participants would "figure out" how to use it themselves. It was then "free for all" to explore the application and get into the exercises. The game consisted of nine exercises in five different categories, amounting to 1000 points. The users started with 0 points and the skill level "Novice". Upon reaching 500 points, they would gain the "Intermediate" level, and when reaching 1000 points, they would become "Expert". The testing lasted for approximately 45 minutes.

After everyone had finished the testing, there was a general discussion of the experience, where the participants were encouraged to discuss the concept and give feedback to how they liked the application. They were also asked if they had paid attention or recognised some of the gamification elements. The last 20 minutes of the workshop were scheduled for answering a questionnaire. The answers were submitted anonymously through a web form. Table 4.4 shows the general topics of the questions. The actual questions are given in Appendix C. The results are given in Section 5.3.

4.3 Data Analysis Method

In the first workshop, sound recording was used to support the notes, and in the second workshop, most of the results were gathered through the questionnaire at the end. Beyond that, the data were recorded with pen and paper. Immediately after each session, interview or workshop, the collected data were rewritten in summary sheets, along with memos of the impressions or other thoughts obtained during the session, as recommended by Robson [2011]. Within the first day after each session, the results were transcribed and put into context as results for the study. This involved a further compression and compilation of the data conforming to the topics

Table 4.4: Topics that were discussed in the second workshop.

Topic	Motive
Motivation for training and compliance	Assess whether gamified training is more engaging, and if it can result in improved learning outcomes. Also, evaluate whether it could lead to behaviour change.
Voluntary use	Determine if the application could be used voluntarily.
General feedback and suggestions	Receive feedback on the overall impression of the application and pointers on how it might be improved.

that were selected as focus points for the individual session (as given in Table 4.2, Table 4.3, and Table 4.4). Additionally, after the interviews and the first workshop, an interim summary was produced in order to create the basis for the prototype development. Since the data collection was run concurrently at two companies, the results were further processed to allow comparison of how different subjects were regarded by the two companies. However, if the representatives from both companies had corresponding views, they were registered as one result. Furthermore, since the workshops generated a high amount of data, some results have been omitted. It was prioritised to report on opinions that were mentioned by more than one person. Finally, after each session instance (interviews, workshop 1, or workshop 2) had been completed for each company, the results were registered as given in the next chapter. The results are further analysed and discussed in Chapter 6.

Chapter 5
Data Collection Results

This chapter presents the results from the data collection. Starting with the interviews, the results are presented in the chronological in which they were collected. It is however important to note that the results from the second workshop are largely dependent on the prototype (as presented in Chapter 3), while the prototype itself is based on the results of the interviews and the first workshop.

5.1 Interviews

Topic 1: Information security awareness and training

Challenges The challenge with security behaviour is that employees may not always understand the real risks connected with security breaches—and there are two main reasons for that: (1) a fundamental lack of competence on the subject, and (2) that security breaches do not directly affect themselves. An example here was that for other fields where employees are required to have awareness and competence, such as Health and Safety Environment (HSE), people are more motivated to engage in the training, because failure to comply with those policies can result in personal injury.

An interesting point made by interviewees at both companies was that a common misconception among many employees, is that security behaviour is "something special", that it is a separate kind of company culture. This can be because security periodically receives high attention and falls in the background typically until "the next campaign". Ideally, good security behaviour should just be a subset of the overall company culture and not be viewed as an autonomous exercise or responsibility.

Interviewees at company B said that another common problem is that security management may lack the ability to correctly convey the security message—which is a rather pedagogical issue. It is therefore essential that management first survey the current state of the employees before the training is initiated. Moreover, management

may have a tendency to underestimate how long it actually takes to change behaviour, and that they may not know how it is best achieved. Behaviour change is a time consuming task that requires repetition and maturing before seeing actual results.

Elements of success Training needs to incorporate material that is as relevant and personalised as possible for the target audience. Examples mentioned here were: (1) use of analogies to make the material more relatable for the recipients, (2) use of real stories (e.g., news stories) that describe security events and/or consequences of security breaches, and (3) make the information *tangible*, i.e. describe it in a way that people understand and can visualise.

Company B interviewees also said that it is necessary to take a layered approach to the training. There must be a fundamental perception of different security aspects among the employees before it becomes practical to commence any form of education. It is also important to clarify *how* social engineering attacks work, in order to highlight the sophistication of today's attacks—and thus what to look out for. Additionally, it can be useful to include interactive exercises where employees are able to actively participate in the training, or to run real life simulations of social engineering attacks, such as phishing scams.

Social norms and persistent behavioural expectations can also be a powerful way of creating the desired security culture, especially for new employees. Over time, this will help to create good habits among the employees to practice favourable security behaviour. Furthermore, company A interviewees added that one should try to a establish an internal company brand for good security culture; a brand that employees will associate with something positive, and that can create a "talk of the office". It is also important to continually receive feedback from the employees in order to efficiently adapt the training to their needs and capabilities. Training also has a tendency to be too lengthy, resulting in that people will try to avoid it or put it off until the last minute. And lastly, current training methods are too often lacking a proper way of measuring the effects of various activities on the actual security behaviour.

Core issue Lack of general awareness is the cause of most security breaches, and thus programs should first and foremost be focusing on this level of knowledge. However, it was emphasised by the interviewees that different job roles, especially with regard to different levels of privilege, will often require other appropriate materials. Furthermore, it is just as important to make the material relevant for the actual company as a whole, e.g., with respect to actual policies and software that is used.

Topic 2: Gamification

Potential Regarding the use of gamification in general, the interviewees said that it could in some ways rejuvenate security training—and help to eliminate the tediousness by providing some of the motivational aspects that security training is currently missing. It was also pointed out that a gamified solution could in fact be a suitable way of blending security in with other subjects, such that it could be a platform for delivering training in several different topics, defeating the disconnected view it has today. Furthermore, gamification could help to create a kind of "security community" in the workplace, which would be beneficial for the reputation of security in general among employees.

Shared goals The business objectives related to security training are to ensure that employees handle sensitive information in a way that does not lay the ground for loss or disclosure of that information—as a result of a security breach. It is therefore important that the management communicate and highlight the advantages of security, and show that it is a vital part of the company's culture and values. It is assumed that it is in everyone's best interest to work in line with those values. A serious security breach can have consequences for the employees as much as for the business itself, especially when it comes to financial losses. Contrarily, a universal objective is to retain an enjoyable atmosphere at work. Thus, if gamification can help to make security awareness and training entertaining and pleasurable, it would reinforce that objective. Moreover, as added by a company A interviewee: good security behaviour is usually something that employees also will need in order to safely interact with IT systems outside of work. By incorporating good practices at work, one will also be more aware of security risks at home or on travels.

Topic 3: Long-term and continuous training

Concerns Content development, growth and relevance will be key concerns for a long-term training solution. The interviewees at company A suggested that companies could be encouraged to create their own content. This would ensure frequent updates and content that is relevant for the respective policies and systems. This could either be done by management or by "superusers" in the application. However, as this would be a rather ideal situation, interviewees at company B emphasised that, it will depend largely on the security focus of the relevant company. For example, some companies will not see the value or will not have the resources to implement custom content.

Furthermore, application security and user privacy are important aspects to consider when developing a solution as the one proposed in this thesis. Measures must be taken to secure the data that is generated by the application, as it will potentially uncover the actual security posture of the relevant company, in terms of

what employees are good at—*and not good at*. However, the interviewees answered that it is indeed possible to accomplish. If the application is to be hosted by a third-party provider, then data should only be stored in such a way that it is of no value to others, and such that only the relevant company has the ability to decode and make sense of the data. This involves not only encryption, but also ways to obscure the relations in the database, and ensure that there is effectively no link between the actual data and the company from which it originates. Players should probably also use aliases or nicknames instead of real names.

Metrics Lastly, a long-term program will be a source of comprehensive performance metrics. The interviewees said that they constitute a great way to locate weak spots, enabling focused campaigns to remedy particular weaknesses. Company A interviewees added that it is very valuable to find the correlation between particular activities and increased performance, but that it can be a challenge to calculate this correctly. Company B interviewees emphasised that this is in fact very sensitive data, but as long as the weaknesses are handled within a reasonable time frame, it could alleviate value of the data to others.

5.2 Workshop 1

Topic 1: Pros and cons with existing training solutions

Pros	**Videos** were mentioned as a good way of delivering information. However, it was emphasised that they should be concise, and *not* contain control questions.
	Interactive exercises, such as incident simulations and quizzes, were said to be informative and not-so-tedious, as an improvement over reading long security guideline-documents.
	Humour was mentioned as a factor that alleviates the tiresomeness often connected with security training.
Cons	**Repetitiveness** was mentioned as a negative factor; the tediousness of repeating the same exercises; there is nothing new to learn, but it is still mandatory to do it. The exercises and content needs to be rejuvenated from time to time.
	Generalised content can be disengaging and tedious as it often fails to connect the information to the recipient's actual work tasks and processes.
	A sense of progression is missing. Upon completing training, one would typically receive a status of "complete" or "incomplete" on the training. This does not provide the user with a perception that he or she actually has learned something or gained new skills.
	Too long training exercises. The exercises should be succinct and frequent rather than long and seldom. This way there is more flexibility concerning time scheduling and it is also easier to remember the material.
	Explaining *why*: it is important to back up training content with logical reasoning, such that is is easy to understand why certain work processes are regulated by security.

Topic 2: Shared goals

The discussions revealed similar thoughts in both groups. The first thing that was brought up was that *nobody wants a computer virus*. Moreover, nobody wants to be *guilty* in causing a security breach; there would be a feeling of guilt or shame if one's actions would cause loss or disclosure of sensitive information. It was also explained that employees generally wants the best for their company, and that a good security posture is important for the company's reputation. Additionally, projects also have value for the employees in the sense that they have put a lot of time and effort into it, and thus loss or devaluation of this work will have a personal impact. Furthermore,

it was claimed that employees are normally open to learn new things; employees are eager to gain new knowledge as long as it is appears relevant for their work, and is presented in a informative and engaging form. Lastly, it was was mentioned that receiving security training at work is also beneficial for safe interaction with IT systems on a private basis.

Topic 3: Motivational factors; game economy

The participants were introduced to the game economy (Figure 2.4), and were asked to take a few minutes to choose five of these motivational factors that they would consider to be the most important in a gamified SAT solution. The results were submitted to a web form, and then discussed in plenary.

Group A answers

1.	**2.**	**3.**	**4.**	**5.**
Prizes	Cash	*Mastery*	Discovery	Status
Mastery	Discovery	Friends	Status	Leadership
Progression	Leadership	Excitement	Likes	Rewards
Excitement	Progression	Discovery	*Mastery*	Points
Friends	Surprise	*Mastery*	Progression	Status

The answers from group A prominently feature factors from the *self-esteem* and *social capital* sections. *Mastery* is the factor mentioned by most. This was explained with the need to feel that the training has a purpose, and that completing it has a challenge to it that leads to a sense of achievement—or mastery. It was however also emphasised by two participants that some would maybe prefer physical rewards more than virtual goods; at least that the final prize is something tangible. Examples here were some form of collectibles or other practical items such as coffee mugs or t-shirts.

Group B answers

1.	**2.**	**3.**	**4.**	**5.**
Discovery	Excitement	*Progression*	Mastery	Groups
Rewards	*Progression*	Praise	Excitement	Status
Points	Rewards	Levels	*Progression*	Conquest
Progression	Mastery	Resources	Discovery	Excitement
Progression	Leadership	Surprise	Discovery	Rewards

The answers from group B show a clear indication that the users value *Progression* as a motivational factor. This was justified by the wish of getting feedback from the training—some form of confirmation that you have completed something, or that you are in fact moving towards some goal. Another highly rated factor was *Discovery*. This was explained by the desire to discover new knowledge and learn new things. As with group B, it was mentioned by two of the participants that there should be a reward for the winner, with an emphasis on extrinsic prizes.

Additionally, both groups declared that there is a significant value in the use of social media components. Interaction with other colleagues, e.g., share accomplishments, compare ratings and engage in collaborative challenges are strong motivational triggers. Moreover, it is more encouraging to engage in something that others also do and care about.

5.3 Workshop 2

Topic 1: Motivation for training and compliance

As part of the questionnaire, the participants were asked to answer the following three questions:

1. Was your impression that the use of gamification can lead to *more motivation* towards completion of the training?
2. Do you think that the use of gamification can lead to *improved learning outcomes* from the training?
3. Do you think that the use of an application like this would make you *think more about security* when at work?

All the participants answered *yes* to the first and third question. Nearly all answered *yes* to the second question as well, however two participants at company A said that they were not sure whether the actual learning outcomes would be improved, but emphasised that they would probably pay more attention during the training as it would be less tedious, and that the use of gamification could help reduce the battle of repeating the training. Beyond that, the participants justified their answers by identifying the following attributes:

- **Progression:** Continuous track of progress in terms of levels, points and leaderboard ranking would create a sense of individual progression—and that "you are in fact increasing your knowledge/intellect".
- **Competition:** Elements such as the leaderboard would spark competition between co-workers. It was however pointed out by some participants that competition may not resolve as an engaging feature for all people.
- **Interactiveness:** High level of interactiveness was said to defeat some tediousness (more motivation) and also lead to more concentration—as in improved learning outcomes.
- **Conciseness:** Short and compact exercises that do not require any particular allocation of time in order to complete. Learning outcomes could be improved in the way that you would get served "small portions of information" at a time.
- **Accessibility:** Related to the conciseness, the ability to commence the training "when you feel like it" was mentioned as a sense of freedom that would lead to a more positive attitude towards the training as a whole. Also, the fact that the training is more likely to be "spread out" can result in a higher awareness and longer-lived mindset towards always-on-security.

Topic 2: Voluntary use

The participants were also asked to consider whether they would use the application voluntarily. Interestingly, the answers at company A and B were quite dissimilar. The majority of participants at company A said that they would consider using the application voluntarily some minutes per day (though this was indicated to be of competitive reasons). At company B, the participants were quite clear in that they probably would not use the application voluntarily without any requirement from the management. One participant pointed out that even though it is interesting, it would still feel like work. The participants agreed that there should be periodic campaigns where everyone would be required to achieve a certain amount of points before some deadline. They emphasised that the gamified training is more engaging, and that a minimum requirement of points would not negatively affect that. It was also mentioned as important that there is some promotion and hype of the application in the workplace and internal communication channels.

Topic 3: General feedback and suggestions

The general opinion in both groups was that the application was well arranged and perspicuous; easy to navigate and that it gave a clear view of the categories that are comprised in the field of security (at least what is relevant for employees). It was easy to track the progress in terms of levels, points and leaderboard ranking.

With regard to the most/least engaging type of exercise, the opinions were rather diverse. There were however multiple participants at company A who pointed out that the most engaging thing about the exercises was the variety itself; that different types of exercises as a whole made the application more interesting. It was also mentioned that is was liberating to be able to individually choose training topics, and that one could mix them freely. Another interesting observation was that group A were very eager to try out the "challenge-a-colleague" functionality (even though it was not yet implemented), while group B did not seem triggered by this at all.

Conclusively, the participants provided multiple individual suggestions for improvement of the application and the concept itself:

- Use of sounds and notifications.
- More social components such as the ability to leave comments on tasks and reach to other peoples' achievements.
- There should be a clearer path to how you are supposed to build you skill level. For example, you could be required to reach a certain skill level before you can embark on the higher level tasks. This would assure that prerequisite knowledge is correctly acquired, and that there is an even clearer process in the levelling schedule.

- Upon doing a quiz, there should be a deduction of points if you answer a question wrong, such that it is not possible to "just guess" and still receive the full amount of points. This would lead users to be more focused, as you would be careful not to lose points.
- The application should in some way take into account the user's previous knowledge.

Chapter 6
Discussion

This chapter leads a discussion on the use of gamification in security awareness and training programs. Based on the literature review in Chapter 2, the concept and prototype presented in Chapter 3, and the results in the previous chapter, it is attempted to answer the research questions, and infer if and how gamification should be used. Conclusively follows an evaluation of the study and the validity of the results.

6.1 The Goals

One of the most integral building blocks of gamified solutions are the *goals*. Gamification should be used as a tool to construct a path that will lead employees to reach their goals [Burke, 2014]. This is the background for research question 1: *How can good security behaviour be viewed as an advantage in the eyes of the employee?* Both the interviewees and the workshop participants (WPs) were asked to identify what the goals with security awareness and training are, i.e. why should employees care about it? On a high level, the goals on the company side are typically something along the lines of (1) operating without security breaches, (2) cultivating good security practices and policy compliance, and (3) maintaining a good reputation for the company outwards. However, the goals on the employee side are not so definitive, as people will undeniably have different views on that. Still, both the interviewees and the workshop participants managed to come up with some rigid suggestions for goals that can be common for both the company and the employees in it.

Business prosperity First off, both interviewees and WPs suggested that training is important to secure the business, in the sense that all parties generally wants the business to go well. The WPs also said that they would feel *guilty* if their actions would cause a security breach. Moreover, it was mentioned that the work they have done and data they have produced has personal value, in the sense that many hours of work and dedication has been put into it. It will therefore be important

in a SAT program to thoroughly explain the consequences of a security breach—i.e. create awareness. The interviewees also emphasised that it is essential to explain the workings and sophistication of social engineering attacks.

Work gratification Suggested by the interviewees, perhaps a more primitive goal, but yet important: "if gamification can make the security awareness and training an *enjoyable* exercise, this could enforce a more positive workplace environment". If it could be so, that the security training would lead to contentment in the workplace, in the way that employees will have a positive experience with the training and feel more satisfied; then this can turn out to be one of the most meaningful goals. Even though this goal was not explicitly mentioned by the WPs, they said that the training would be more motivating when gamification was used. It was also apparent that workshop group A was very excited by the "Challenge-a-colleague" feature. Furthermore, some WPs suggested in the first workshop that *humour* (synonymous to joyfulness[1]) was a favoured factor in the existing solutions they had seen. Tsohou et al. [2015] also recommended that security awareness material should incorporate *positive stimuli*—e.g. humour. Consequently, the use of some comedy in the solution should not be underestimated.

Competence growth Another goal that was suggested by the WPs was that "employees are generally eager to learn new things and increase their competence", in the sense that if security appears as an important part of their work, they would be motivated to learn about it. Additionally, both interviewees and WPs argued that "security awareness and competence is something one would also need outside of work, e.g. while browsing the web at home". This could be an important motivator, as information security is regularly getting increased media publicity, highlighting that people should watch out for threats.

Clear reasons There is one matter that has come up several times in this study; Siponen [2000], ENISA [2010], in the interviews, and in the workshops: that it is very important to explain why some practices and processes are regulated by security. For example, not just say "you cannot connect USB thumbdrives to your company computer". It is necessary to explain the reason for that as well. Even though it was not mentioned as a *goal* per se, by neither interviewees nor WPs, it appears to be something surely beneficial for both the company and the employees: explaining—and knowing *why*. Getting the explanation may have significant impact in employees towards compliance with regulations. This may also affect the perceived risks of security breaches.

[1] Synonyms from Thesaurus.com; http://www.thesaurus.com (Dictionary.com, LLC. 2016.)

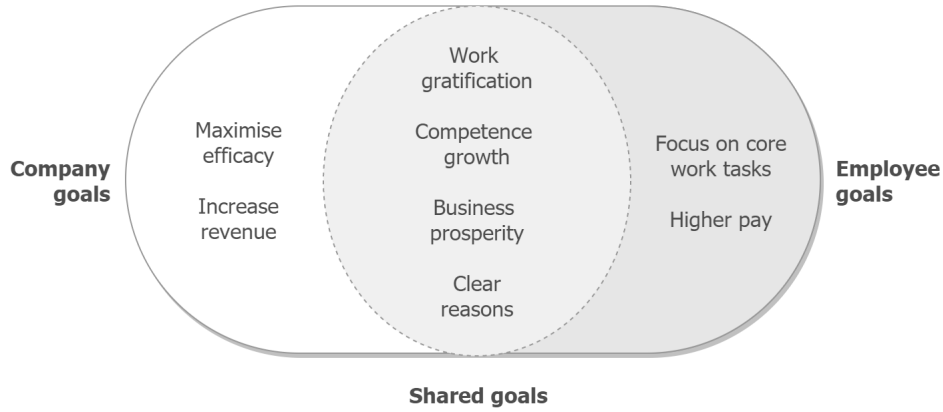


Figure 6.1: A Venn-diagram with company goals and employee goals.

Figure 6.1 shows a Venn-diagram that illustrates the overlap of company and employee goals. Also present are some sample extremity goals for each of the two entities to illustrate typical goals that are not shared between the two. It should however be argued that some goals, particularly "business prosperity" and "competence growth", are based on the premise that the respective employee already inhabits the *awareness* of security and recognise that security threats are real—which in this study was the case for all WPs. In a company where employees do not even *perceive* [Shaw et al., 2009] security, this would probably not be goals they would consider. Furthermore, it is not clear to which lengths an employee would go to ensure that they know what they need to know about security, especially if their *perceived risk of security incidents* [Tsohou et al., 2015] is low.

6.2 The Motivation

Fundamentally, the purpose of gamification is to increase motivation [Burke, 2014]. At the same time, motivation is arguably one of the main challenges in security awareness and training; motivation to learn and motivation to act. This calls for research question 2: *Which motivational factors are the most important in a security awareness and training program?*

6.2.1 Progression

In the first workshop, the participants tabulated a series of factors that they had experienced as pros and cons in previous training solutions. They also defined what they considered to be the most important motivators to be used in a security awareness and training solution. One of the recurring factors was *progression*. It was said that a sense of advancement and accomplishment is usually something that is

missing in current solutions. Completed training is often just recognised by a status change (e.g., from "incomplete" to "complete"). The feeling of progression would naturally be something that people perceive differently, however in a general sense, one might argue that it could be triggered by two things: (1; internal) a feeling that you have "used your brain" to process information or to solve exercises that you had not encountered before, and (2; external) getting feedback from some source that acknowledges your efforts and tells you that you have successfully completed something—that you are moving closer to your goal.

Supporting the first claim, Puhakainen and Siponen [2010] discovered that successful training solutions should in fact account for the learners previous knowledge; and present the material in ways that will trigger cognitive processes with the learner. However, this requires careful design of the actual content; the material that is presented. Thus, training programs should incorporate methods for assessing what the learner already knows, including processes for efficiently handling the repetitiveness of the content. This may however turn out to be a taxing process that could require a good deal of resources. The challenges related to this are further addressed in Section 6.4. As for the feedback, this is where the gamification steps in. First of all, the basics: points, levels, and achievements represent a trivial way of recognising someone's endeavours. However it does not—and should not—stop there (avoiding the "PBL-triad" [Werbach and Hunter, 2012]). Progression can be relative—i.e. relative to others; other players. Social capital was presented by Burke [2014] as one strong motivational factor; the ability to share and *compare* your achievements with your peers. Maslow [1943] said that one of the basic needs for human motivation (as part of Maslow's hierarchy of needs) is the *esteem*; self-esteem and esteem of others. Social esteem, receiving feedback in the form of recognition, attention, and appreciation from other people are strong motivational drivers. Therefore, the use of social interaction is important in a gamified application. The technology (i.e. the Internet) allows this element to be easily integrated into any gamified platform. The prototype presented in this thesis used such social triggers in elements like the leaderboard, where people could compare their scores, and the activity timeline, where players could view their own and other players' achievements. For example, the answers to the questionnaire in workshop 2 featured comments like: "It was fun to track people on the leaderboard", and "It was nice to follow the other players' progressions on the activity timeline."

6.2.2 Security Culture

The prospect of social interaction also has other sides to it. Chapter 2 presented a series of challenges related to the process of security awareness and training, specifically when it comes to factors that affect the employees' ultimate compliance with security policies and regulations (Table 2.1). Among them were "normative

beliefs", "social pressure", and "habits" [Tsohou et al., 2015]. During the interviews it was put forward that "security is often viewed by employees as a *separate* concern from all else that comprises the company *culture*". The company culture typically consists of a manifold of behavioural expectations and normative beliefs that employees in the respective company possess and follow; just like "that is how things are done here". Good security behaviour needs to be a part of that; the culture and the norms. One example that is featured repeatedly in the gamification literature is the program called Opower [2016], that uses the social aspects of gamification to reduce people's power consumption. In short, Opower lets people compare their electricity usage with the one of their neighbours; with statistical overviews and feedbacks upon low consumption etc. If you use more electricity than your neighbours, you would possibly feel like you are deviating from an expected group behaviour [Burke, 2014]. Opower utilises the fact that people often want to align their behaviours with a group's social norms—which in this case would be to save energy. As result, it has helped save over 9,6 billion kWh of electricity in the U.S. (as of May 2016) [Opower, 2016]. However, it is not to be ignored that introducing new social norms and behavioural expectations can be a tricky affair. Thus, following from the interviews, it was advocated that good security behaviour could advantageously be associated with something like a brand, as a means to create attention around the security culture. A successful branding of good security behaviour, with the use of a gamified training application, could possibly help to attain the recognition that security needs, and, as suggested by a WP, for example create a topic for the occasional small talk around the coffee machine or in the elevator.

6.2.3 Competition

Elements like the leaderboard and activity timeline let the players compare their progress and achievements. For many people, comparison will almost instinctively evolve into *competition*. And competition can be a source of great engagement. However, as Burke [2014] points out: "In gamification, we most often want everyone to win". This is certainly true for security awareness and training; the objective is to educate everyone. Consequently, introducing competition into gamified solutions, especially as the one considered in this thesis, can be risky. When using competition based elements, it is important to balance them, and also let people opt-out. One feature in the prototype that was honoured by the WPs, was the ability to filter the leaderboard, such that you can choose with whom you are competing. This way, if a player ranks low on the global leaderboard, they may still be competitive in their department or among their friends. Other players may choose not to follow the leaderboard at all. The activity timeline has a similar filtering mechanism. One WP emphasised that they would receive sufficient motivation from simply tracking their own progress. Still, comments from the second workshop included:

"Competitions would probably make me use the application more frequently.", and "Challenge-a-colleague needs to be implemented!"

It is not easy to anticipate exactly how people will react to different competitive elements within an application. Some might find it engaging, some might find it demotivating. An important aspect will however be that players can choose which competitive level they wish to be on. Burke [2014] suggests that an alternative way of creating competition is by using a "collaborative-competitive" approach, where people are competing as teams rather than as individuals. Building on the team spirit, it could create a more healthy form of competition, where people would fight for their team, and potentially lose as a team, which is a softer way of losing than if you are alone.

6.2.4 Self-Determination

As described in Chapter 2, the Self-Determination Theory (SDT) defines three factors as fundamental for intrinsic motivation: competence, autonomy and relatedness. Competence is in many ways the same as mastery, and in the first workshop, this was the factor that was mentioned by most participants in group A to drive motivation. It was argued that the presented material should represent some form of challenge, some impression of interference that must be overcome. Similar to the feeling of progression, mastery could be affected by both internal and external forces. The solution needs to correctly assess the user's skill level in order to create a reasonable degree of challenge. Concurrently, mastery can be achieved with the use of points, levels and achievements, in that the player has "mastered" a level, or unlocked an achievement that few others have. Moreover, mastery can be enforced by the use of positive words, such as "excellent", "awesome", or "good job". In the prototype, this was used when a player had completed an exercise, or reached a new level. This contributes to let the player know that the efforts had meaning and that they indeed were accomplishments Werbach and Hunter [2012]. Furthermore, Deci [1971] found that external rewards like positive reinforcements can increase the intrinsic motivation in the activity. The second intrinsic factor in SDT, autonomy, means that people should have independence and freedom to make their own choices. For gamification this typically means that the players are able to act freely in the play space (at least to some degree). In the prototype, the WPs were able to for example choose whether they wanted to take all the exercises in the password category in one go, or if they wanted to mix tasks from several categories. Additionally, as opposed to regular security awareness and training (e.g., traditional e-learning), the concept of this thesis further promotes autonomy by letting employees control their training in terms of time, location and duration. Short and compact exercises means that training can be divided up in five minute intervals that can be freely distributed. The third and final factor of intrinsic motivation, relatedness, has already been discussed

as part of the shared goals, in that the security training is important for business prosperity and development of personal intellect. Furthermore, relatedness is also affected by the social aspects that were discussed earlier in this section.

Summarily, Figure 6.2 depicts an approximation; an intuition, based on the results from the study, of how security awareness and training fits into the SDT continuum (here illustrated as a radar chart)—with and without use of gamification. First without gamification, the intuition is that security awareness and training is something people do not do out of pure joy; i.e. low intrinsic motivation. It is however something that relies heavily on extrinsic motivation; especially the external regulation. The training is something employees *must* do. Next, it is to some degree motivated by introjection, because some people will acknowledge that middle management needs to be able to check off on compliance (greater cause). Others might do it so that they can answer yes to the question "did you complete the security training?". Likewise, it can be influenced by identified regulation in the way that people do in fact think that security training is to some extent necessary, and that it has some value. To a modest extent, it can also be influenced by integrated regulation because some people want to know what the security regulations are, and think that it is smart to be aware of them. Lastly, some people could actually do the training under amotivation in the sense that they could do it merely without even thinking, the "just click through it without paying attention".

Subsequently, when introducing gamification, the approximation is slightly changed. It is assumed that the fulfilment of competence, autonomy, and relatedness will bump up the intrinsic motivation to some extent. Based on the results from the second workshop, it appeared that the participants were more positive to the gamified solution—maybe for some it could even be fun. In the extrinsic spectrum, it is assumed that because it becomes more self-determined, the external regulation factor is reduced: it is no longer merely an activity of compliance. It is further assumed that the introjected regulation is increased as a result of the social aspects induced with gamification, that completion of the training is something that is recognised by other employees. Contrarily, gamification is not seen as to have any particular effect on either the identified nor the integrated regulated motivators. Even though the training is more motivating in itself, it does not appear that security is considered as more *valuable* or important to the individual employee. However, if one could manage to adequately adapt the content to accommodate the individual employee, it could result in people feeling like the training is of more importance. This could also be affected by introducing clear reasons for the security regulations, as discussed in Section 6.1.

Figure 6.2: Positioning security awareness and training in the SDT with and without use of gamification. Whole line represents with gamification; dashed line without.

6.3 The Endurance

One of the main ideas considered in this study is that of having a long-term and continuous training program, with small exercises that are short in content and duration. This would allow the employees to distribute the training according to their own preferences, and complete the training on their own terms. This leads to research question 3: *What are the possibilities and limitations of a long-term, gamified security awareness and training program?*

6.3.1 Learning Outcomes

As with any educational program, the purpose of a SAT program is to facilitate meaningful and memorable learning outcomes for the employees. Shaw et al. [2009] concluded that hypermedia, or online media, with the use of elements such as interactivity, adaptability, social learning, convenience, and instant feedback, have

positive correlations with improvement of security awareness. The results from this study, particularly from the second workshop, indicate the same—i.e. that gamification can be a useful tool in creating improved learning outcomes for SAT programs. This can be explained by (1) reduced tediousness of the training, such that one might pay more attention during the training, (2) more motivation towards completing the training, that is, people are not so reluctant to actually doing it, and (3) conciseness and availability of the exercises, such that employees are free to do the training when when they want and also spread it out over a longer time period. Although already mentioned as a motivational factor, the latter argument also conforms to what is known as the spacing effect; that learning is greater when the training is spread out over time [Wikipedia, 2016b]. This particular principle is also used by the Norwegian e-learning vendor Junglemap [2016]. They use this feature, which they call "NanoLearning", in several e-learning programs, one of which is security awareness. Junglemap was profiled in the 2015 Gartner Group Magic Quadrant for Information Security Awareness [Walls, 2015], where the short duration courses were attributed as a strength.

6.3.2 Performance Metrics

Another aspect that follows from long-term, gamified training, are performance metrics. Although this was not a centre of focus for this thesis, it was mentioned in the interviews that current training methods are normally lacking proper monitoring and evaluation of the actual effects of the programs. Bada et al. [2015] mentioned this to be one of the factors leading to the failure of a SAT program. Kruger and Kearney [2006] emphasised that measurement of effectiveness adds significant value to a program, and recommended that there should be automatic methods for doing this. Moreover, it was highlighted that measurements should be done on a low level, in order to accurately discover where awareness is lacking. With a program such as the one proposed in this thesis, all of this is in fact obtainable. Metrics can be automatically generated when people use the application. For example, it can be possible to discover which task types are the most popular, by looking at which tasks the players choose to do first. Furthermore, knowledge can be measured by assessing levels between tasks. This would also allow an assessment of which tasks that are actually the most effective conveyors of knowledge. As mentioned in the interviews, metrics can also be used to locate areas where employees show weak performance, and thus allow focused campaigns to patch up those. Eventually, performance metrics can be analysed in numerous ways, and it would be up to each individual company to decide how to use them.

6.3.3 Behaviour Change

As part of the second workshop results, the WPs indicated that the use of a long-term gamified SAT program might make them think more about security at work, which in principle indicates a change in behaviour. This was also said to be an attribute of the idea of using short exercises, as the training could turn into a daily or weekly activity, rather than for example a once-a-year effort.

6.4 The Limitations and Challenges

The combination of the goals, the motivation, and the endurance discussed here point to a positive potential of using gamification in the program. However, following the second part of research question 3, there are also some limitations and fundamental challenges related to use of gamification in SAT.

6.4.1 One Program to Train Them All

- "The most successful programs are those that users feel are relevant to the subject matter and issues presented." [NIST, 2003]
- "It is critical to segment audiences and ensure that people only receive the messages they need. A one-size-fits-all strategy might be easier to develop and implement, but it will not be effective." [ENISA, 2010]

The guidelines are unambiguous: a SAT program needs to be designed with the target audience in mind. This is a major challenge that applies to any SAT program. It was pointed out in the first workshop that content that did not appear relevant to the work of the individual employee only had a demotivating effect. Based on the conclusions of Puhakainen and Siponen [2010] (Section 2.1.2) and recommendations from NIST [2003], together with opinions collected from the interviews, it is assumed that the two most important factors are (1) to take into account are previous knowledge, and (2) to adapt the content to fit job roles and responsibilities.

The intuition is that gamification in itself cannot explicitly simplify the process of delivering the right content to the right people. However, small and concise exercises allows to more easily segregate the content into different blocks or components of exercises that can be served to people with different job roles. In order to handle previous knowledge, there could be an introductory assessment, e.g. a quiz that touches on several subjects, that establishes an understanding of the current competence level of every new user. The user could then be assigned blocks of exercises accustomed to their current level of knowledge.

Unfortunately, the challenge of having one program for all employees will actually escalate further when using gamification. Bartle [1996] introduced the theory of

player types, where three distinct types of game players were defined: explorers, socialisers, achievers, and killers. This means that one might in fact see players that are playing for completely different reasons. Explorers will analyse, examine and test out all features of the game, trying to get a comprehensive view of how it all works. The socialisers are playing mostly to connect with other people; to chat, help others—and just socialise. The achievers on the other hand are focused on the achievements, the points, and the levels; getting to the top—winning the game. Lastly, the killers. They are perhaps even more competitive than the achievers in the way that they often will try to eliminate other players while making their way to the top. As a consequence of the various player types that may emerge, it is necessary to design the gamified application to accommodate them all.

6.4.2 Repetitiveness

Another challenge that is fundamental to all SAT programs, is the process of reiteration. A company will typically have periodical (e.g., annual) security programs, where the material is quite similar every time. From the security perspective, that is generally fine, as the employees often need to be aware of the same things from one year to another (perhaps with some alterations). However, as mentioned by the WPs, the repetitiveness can be quite tiresome. As described in Chapter 3, the concept of this thesis involves having regular updates and refreshing of the content. Three main approaches have been considered to alleviate the problem of repetitiveness:

1. Regularly create new tasks of the article type (Section 3.2.1); there are often published new articles on the web that report of security breaches and social engineering attacks.
2. Create tasks with the same content, but presented in different forms, e.g. as different task types.
3. As inspired by Duolingo (Section 3.1.2), repetition can be part of the game. At some point, players will need to refresh their their knowledge to keep their status.

6.4.3 Voluntary use

Burke [2014] says that gamified solutions function best if they are opt-in, i.e. voluntary. Mollick and Rothbard [2013] found that consent correlates with how the use of gamification is perceived in the workplace. Although they could not conclude that consent directly influences the actual performance, their results showed that if there was consent from the employees to engage in the program, then it would improve their positive affect. Similarly, without consent, it would decrease. A topic in the second workshop was to evaluate whether using the training application could be voluntary—implying that people would actually use the application and individually prescribe

to the right amount of training. Even though the opinions were slightly divided between the two groups (answers were both yes and no), it is perhaps most likely that the majority of employees would not use the application if it was unconditionally voluntary. It is important to keep in mind that SAT is still something people *have to do*, it is in fact mandatory. The purpose of using gamification is for the most part to make the training less tedious, and help defeat the negative view that people may have on security (at least on the training) itself—and hopefully, make people learn more, and eventually affect their behaviour. In some cases, employees might also do more training than what is mandatory. A suggestion made by the WPs, was to have periodical campaigns, where a minimum amount of activity is mandatory. This will result in a decrease of autonomy, however people will still be able to control and distribute their own training within the limits of the decided training period.

6.4.4 Other Concerns

Demographics Many companies have employees of different age, culture, and origin. It is not all clear how this will influence the use of gamification. It was however suggested in the workshops that it may turn out to appeal most to younger employees. Moreover, the interpretation of rewards can vary between cultures [Burke, 2014]. It could therefore be an idea to have alternatives to the gamified application for those who would prefer other training methods.

Content depletion Interviewees emphasised that in order to keep players engaged over time, it is important that there is enough content to fill long periods of training. However, for security awareness and competence, there is only so much an employee needs to know. As discussed under the topic of repetitiveness this requires innovation and originality in the way content is presented.

Resources The process of incorporating gamification into the awareness program can be an exigent operation. Not to mention the development of content. It will often come down to how much resources a company have to spend on security training.

Rewards Even though self-esteem and social capital were the most prominent factors valued by the WPs, there were also some that declared that they would receive greater motivation from physical prizes. This is also mentioned by Burke [2014], that people will always have varying preferences when it comes to rewards.

Hype and overuse In the last few years, the use of gamification has boomed, with points and badges popping up in all kinds of services and programs. The concern is that the current popularity gamification is currently seeing will eventually kill off the actual enjoyment it is supposed to give. Bartle [2011] argued that "the more people see of it, the less effective it will be".

6.5 The Evaluation

It is important that the results and the discussion presented here are considered in line with the context in which the study was conducted. As described in Chapter 4, the results are based on the professional opinions of five security experts, and the personal opinions of 10 employees from two Norwegian companies. This thesis should serve to complement the overall research in the areas of security awareness and training, and gamification, and especially the combination between the two. Once further studies have been conducted in this area, one might come closer to a more generalisable result for how gamification should be used in SAT programs.

Regarding internal generalisability, the group at company A consisted of employees from different departments and service lines, which amounted to a well distributed sample of the company. However, the number of participants is not considered high enough to constitute a sufficient representation of the entire company. Likewise, the group from company B consisted of only representatives from the human resources department, which then possibly gives an even narrower sample of the many departments that comprises the company. It is not clear as to which extent the results are internally generalisable, however, further research could benefit from including more participants. Nevertheless, it was considered as an advantage that the workshop groups were small. Further research may therefore consider to use a similar size, and only include more groups. The overall impression was that the workshops worked well. The participants were engaged throughout the entire session, and everyone were active in the discussions. It should however be addressed that there is a possibility that the participants were a little bit over optimistic in their views on gamification, even though it was emphasised that they should not hold back if they had negative opinions about it. Through the questionnaire at the end of the second workshop, participants expressed that the sessions had been highly interesting. The interviews also worked well as a means to collect qualitative data.

Chapter 7
Conclusions

"Every company has a security culture.
The question is just if it is good or bad."
Norwegian National Security Authority [NSM, 2016]

This thesis has considered the use of gamification in security awareness and training programs. Based on the hypothesis that some of the current programs are unsuccessful in providing employees with the needed awareness and training, an alternative concept has been drafted, and a prototype has been developed. In order to assess the usability and feasibility of this concept, qualitative data has been collected through interviews with security experts, and workshops with user groups. The results indicate that gamification can have positive effects when used in a security context.

7.1 Focus on the End User

Security awareness and training programs are demanding, both for those who make them and for those who take them. The programs are supposed to create awareness, understanding, and competence in the field of information security for people who inhabit a wide variety of previous knowledge. That includes people with no experience, people who already know a lot—and even people who think they already know a lot. In many ways, the key word here is *people*, and that is why this study has focused largely on how gamification could and should be used to make security training a little bit better for *people*.

Through the study, it has been found that many of the problems that SAT is currently facing, are problems that gamification is created to solve. The gamification design process has the end user in focus: why should the employee be interested in SAT? The study discovered four reasons for this, through the shared goals that were identified. It is necessary that programs are constructed fulfil those goals. Another important question is: what drives the employees' engagement? It is essential to

identify how employees are motivated, and it was found that progression and mastery are two of the most important ingredients for that. Additionally, the more self-determined the training is, the more motivating it will be. Another result was that competition can be engaging for many, but also demotivating for others. When the purpose of the solution is to educate everyone on an equal level, it is important to use competition with caution.

7.2 Take Less, More Often

A general opinion among the workshop participants was that current training courses are too long. An important aspect that was considered in this thesis is the use of small, concise exercises, as opposed to hour-long e-learning courses. It was discovered that this feature can give two important outcomes: (1) provide the users with a sense of autonomy about the training, and (2) improved learning outcomes due to the spacing effect, and that the threshold for commencing the training is lower, when it does not require planning—it can be done on the go, when there is time.

7.3 Infiltrate the Culture

Ultimately, the whole purpose of a SAT program is to create behaviour—(good) security behaviour. There is probably no better way of doing this than to make security a part of the culture. There are certain things that employees do because they are following social norms, the behavioural expectations of the organisation, and good security behaviour should be among those things. However, infiltrating the culture and creating new social norms is not a trivial task. As was pointed out by one of the interviewed security experts: "it takes time". Behaviour change is tough, however, the results from the workshop proposed that, if SAT is something the employees are exposed to frequently, it can at least make users think about security on a more regular basis.

7.4 Further Work

The use of gamification in security awareness and training programs is currently a young and unexplored research area. As information security competence is only becoming increasingly important, it is necessary that this research continues. The results presented in this study are based purely on qualitative data collection methods; most of the data are views, opinions, and impressions. Thus, there are no concrete results that can actually show if gamification will improve the security awareness and training process. It is therefore necessary to study if gamified training is more effective than regular training. This can for example be done by deploying a gamified training application with a user group for a longer period and compare the results

with a control group that only takes the normal training. This can at least give an insight to whether gamification can lead to better learning outcomes. Another interesting output would be to see how often the users would use the application, and if anyone would use it more than what is required. Future research should also try to find efficient ways of assessing employees' current level of knowledge, and explore ways to adapt the training accordingly. It will also be necessary to find good ways of mediating the right training to the right people, in accordance with their job roles and responsibilities.

References

Albrechtsen, E. and Hovden, J. (2010). Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computers & Security*, 29:432–445. Elsevier Ltd.

AngularJS (2016). HTML Enhanced for Web Apps! `https://www.angularjs.org`. Google. Accessed on 02 June 2016.

Apozy (2015). Experience Security Gamification. `https://www.apozy.com`. Apozy Inc. Accessed on 25 January 2016.

Awarity (2015). Awarity—The Human Firewall. `https://www.awarity.at`. Awarity Training Solutions GmbH. Accessed on 25 January 2016.

Bada, M., Sasse, A., and Nurse, J. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, pages 118–131. ResearchGate.

Bartle, R. (1996). Hearts, Clubs, Diamonds, Spades: Players Who Suit MUDs. *Journal of MUD Research*, 1(1):19.

Bartle, R. (2011). Gamification: Too Much of a Good Thing? *Presentation given at Digital Shoreditch 04 May 2011.* Accessed on 11 June 2016.

Baxter, R. J., Holderness, D. K., and Wood, D. A. (2015). Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field. *Journal of Information Systems.* American Accounting Association.

BeOne (2016). Mobile learning: BeOne Ubiq app. `https://www.beonedevelopment.com/solutions/mobile-learning`. Accessed on 21 May 2016.

Bootstrap (2016). Grid System. `http://getbootstrap.com/css`. Bootstrap. Accessed on 02 June 2016.

Burke, B. (2012). Gamification Trends and Strategies to Help Prepare for the Future. http://www.gartner.com/webinar/2191918. Webinar. Gartner Inc. Accessed on 20 January 2016.

Burke, B. (2014). *Gamify: How Gamification Motivates People to Do Extraordinary Things*. Bibliomotion.

Check Point (2015). Security Report. Check Point Software Technologies Ltd. Available at `https://www.checkpoint.com/resources/2015securityreport`.

Chou, Y.-K. (2015). Octalysis: Complete Gamification Framework. `http://www.yukaichou.com/gamification-examples/octalysis-complete-gamification-framework`. Yu-Kai Chou. Accessed on 28 May 2016.

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. (2007). A Video Game for Cyber Security Training and Awareness. *Computers & Security*, 26(1):63–72. Elsevier Ltd.

Deci, E. L. (1971). Effects of Externally Mediated Rewards on Intrinsic Motivation. *Journal of personality and Social Psychology*, 18(1):105–115. American Psychological Association.

Deterding, S. (2011). Meaningful Play. Getting "Gamification" Right. *Presentation given at Google Tech Talk 24 January 2011*. Available at `http://codingconduct.cc/meaningful-play`. Accessed on 11 June 2016.

Deterding, S. and Dixon, D. (2011). From Game Design Elements to Gamefulness: Defining "Gamification". *MinTrek 2011*, pages 9–15. ACM.

Duolingo (2016). About Duolingo. `https://www.duolingo.com/press`. Accessed on 24 January 2016.

ENISA (2010). The New Users' Guide: How to Raise Information Security Awareness. European Network and Information Security Agency (ENISA). Available at `https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide`.

EY (2015). Global Information Security Survey. EYGM Limited. Available at `http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity`.

Firebase (2016). App Success Made Simple. `https://firebase.google.com`. Google. Accessed on 02 June 2016.

Hamari, J., Koivisto, J., and Sarsa, H. (2014). Does Gamification Work?–A Literature Review of Empirical Studies on Gamification. *Proceedings of the 47th Hawaii International Conference on System Sciences*. IEEE.

IBM (2014). Cyber Security Intelligence Index. IBM Security Services, IBM Corporation. Available at `http://www.ibm.com/security/data-breach`.

ISF (2015). Medlemsundersøkelse. Norsk informasjonssikkerhetsforum (ISF). Available at `https://www.isf.no/isf-medlemsundersokelse-2015-2`.

Junglemap (2016). About Junglemap. http://www.junglemap.com/AboutUs. Junglemap. Accessed on 30 May 2016.

Khan Academy (2016). Khan Academy: You Can Learn Anything. https://www.khanacademy.org. Khan Academy. Accessed on 13 June 2016.

Kruger, H. A. and Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness. *Computers and Security*, 25(4):289–296. Elsevier Ltd.

Leach, J. (2003). Improving User Security Behaviour. *Computers and Security*, 22(8):685–692. Elsevier.

Maslow, A. H. (1943). A Theory of Human Motivation. *Psychological Review*, 50:370–396. American Psychological Association.

Microsoft (2015). Microsoft Security Intelligence Report. *Volume 17*. Microsoft Corporation. Available at https://www.microsoft.com/sir.

Mollick, E. R. and Rothbard, N. (2013). Mandatory Fun: Gamification and the Impact of Games at Work. *SSRN Electronic Journal*, pages 1–68.

Nike (2016). Come run with us: Nike+. http://www.nike.com/no/en_gb/c/running/nikeplus/gps-app. Nike, Inc. Accessed on 09 May 2016.

NIST (2003). Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. National Institute of Standards and Technology (NIST). Available at http://csrc.nist.gov/publications/nistpubs.

NIST (2013). Special Publication 800-63-2: Electronic Authentication Guideline. Appendix A. National Institute of Standards and Technology (NIST). Available at http://csrc.nist.gov/publications/nistpubs.

Node.js (2016). JavaScript runtime built on Chrome's V8 JavaScript engine. https://nodejs.org/en. Node.js Foundation. Accessed on 13 June 2016.

NSM (2015). Helhetlig IKT-risikobilde. Nasjonal Sikkerhetsmyndighet (NSM). Available at https://www.nsm.stat.no/aktuelt/la-frem-helhetlig-ikt-risikobilde.

NSM (2016). Sikkerhetskultur. https://nsm.stat.no/om-nsm/tjenester/sikkerhetskultur. Nasjonal Sikkerhetsmyndighet (NSM). Accessed on 13 May 2016.

Opower (2016). Elevate your customer experience. https://opower.com. Opower Inc. Accessed on 29 May 2016.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., and Bragge, J. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. *Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006)*, pages 83–106.

Puhakainen, P. P. and Siponen, M. (2010). Improving Employee' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34:757–778.

QuizClash (2016). Our Quiz Games. `http://www.feomedia.com/quiz-games`. FEO Media. Accessed on 24 January 2016.

Robertson, M. (2010). Can't play, won't play. `http://hideandseek.net/2010/10/06/cant-play-wont-play`. Hide and Seek Productions Ltd. Accessed on 11 June 2016.

Robson, C. (2011). *Real World Research*. John Wiley & Sons Ltd, third edition.

Ryan, R. M. and Deci, E. L. (2000). Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. *American Psychologist*, 55(1):68–78. American Psychological Association, Inc.

SANS (2016). Information Security Resources. `https://www.sans.org/information-security`. SANS Institute. Accessed on 13 May 2016.

Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52:92–100. Elsevier Ltd.

Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security*, 8:31–41. Emerald Insight.

Symantec (2016). Internet Security Threat Report. *Volume 21*. Symantec Corporation. Available at `https://www.symantec.com/security-center/threat-report`.

Thornton, D. and Francia, G. (2014). Gamification of Information Systems and Security Training: Issues and Case Studies. *Information Security Education Journal*, 1:16–29. DLINE.

Tsohou, A., Karyda, M., and Kokolakis, S. (2015). Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs. *Computers & Security*, 52:128–141. Elsevier Ltd.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective*, 17(5-6):207–227. Elsevier Ltd.

Walls, A. (2015). Magic Quadrant for Security Awareness Computer-Based Training. Gartner Inc.

Werbach, K. and Hunter, D. (2012). *For the Win: How Game Thinking Can Revolutionize Your Business*. Wharton Digital Press.

Wikipedia (2016a). NoSQL. https://en.wikipedia.org/wiki/NoSQL. Wikimedia Foundation, Inc. Accessed on 02 June 2016.

Wikipedia (2016b). Spacing effect. https://en.wikipedia.org/wiki/Spacing_effect. Wikimedia Foundation, Inc. Accessed on 22 May 2016.

Winkler, I. and Manke, S. (2013). 7 Reasons for Security Awareness Failure. http://www.csoonline.com/article/2133697. CSO Online. Accessed on 10 January 2016.

Zichermann, G. (2011). The Six Rules of Gamification. http://www.gamification.co/2011/11/29/the-six-rules-of-gamification. Gamification Co. Accessed on 28 May 2016.

Appendix A
Interview Outline

The subsequent page includes the interview draft that was issued to the security experts prior to the interview sessions.

Overordnet intervjuplan

Med utgangspunkt i oppgaven ~~(problembeskrivelse vedlagt)~~:

"Use of Gamification in Security Awareness and Training Programs".

Sikkerhetskultur / Security Awareness and Training

1. Utfordringer forbundet med sikkerhetskultur og opplæring.
2. Eksisterende opplæringsmetoder: hva fungerer bra, hva kunne vært annerledes.
3. Mest kritiske kunnskapsnivå (allmenn/generell, rollespesifikk).

Spillifisering / Gamification

4. Mål: bedriftens og brukernes.
5. Faktorer som gjør at gamification egner seg godt til bruk i opplæringsprogram for sikkerhet.

Et langsiktig, kontinuerlig program

6. Praktisk gjennomførbarhet (sikkerhet, personvern, tidsforbruk).
7. Krav som stilles til opplæringsprogrammer.
8. Utvikling og tilpassing av innhold.
9. Logging av bruk.

Appendix B
Workshop Data Collection Plan

The subsequent page includes the data collection plan that was issued to the participants before the workshops.

Plan for data collection

— in connection with Master's thesis: "Use of gamification in security awareness and training programs".

Purpose

The purpose is to collect qualitative data from end users that can:

1. Support the understanding of the current state of IT security awareness,
2. Identify potential positive outcomes of good security behaviour, and
3. Give insight to how a new training approach may be implemented, using gamification as a design technique.

Activities

Activities include a series of two workshops, where the participants are encouraged to actively share and discuss their opinions and views on the topics.

The theme for the first workshop will be *motivation* for practicing good security behaviour. We will assess questions like:

- How does IT security matter to me?
- How can we make IT security training more engaging?
- Where can we find motivation to be more conscious about IT security?

The results will be used to develop a prototype application interface. In the second workshop, we will discuss the design and usability of this prototype.

Timeframe

Duration of the workshops is set to a maximum of two hours each (including a break). This results in a total time of up to four hours per participant.

> ***Gamification***
>
> *«the use of game design elements in non-game contexts»*

Eyvind Garder B. Gjertsen eggjerts@stud.ntnu.no

Appendix C

Questionnaire from the Second Workshop

The subsequent page includes the questionnaire that was answered by the workshop participants as part of the second workshop. The answers were submitted anonymously through a web form.

1. Hvilken oppgavetype likte du best?
   Vennligst begrunn kort hvorfor.

2. Hvilken oppgavetype lite du minst?
   Vennligst begrunn kort hvorfor.

3. Hva likte du med applikasjonen i sin helhet?

4. Hva likte du ikke?

5. Var det noen ting du savnet i applikasjonen?
   Noe som manglet, eller noe som burde vært annerledes.

6. Ville du brukt denne applikasjonen daglig eller ukentlig dersom det var frivillig å bruke den?
   F.eks. 5 minutter om dagen.

7. Virket det mer motiverende å lære om sikkerhet på denne måten?

8. Tror du bruken av "gamification" kunne ført til at du ville fått mer utbytte av opplæringen, enn gjennom andre opplæringsmetoder?

9. Tror du at en slik applikasjon kunne ført til at du ville tenkt mer på sikkerhet når du er på jobb?
   Det vil si, tror du at du ville vært mer oppmerksom på sikkerhet dersom opplæringen ble levert gjennom en slik spillifisert løsning.

10. Hvilke elementer mener du er de viktigste å ha med ved bruk av "gamification"?

11. Var workshop-ene i seg selv interessante?
    1 = Lite intressant, 5 = Veldig interessant