NTNU
Norwegian University of
Science and Technology

Security Risk Assessment in Software Development Projects

Heidi Svendsen

Master of Science in Communication Technology
Submission date: June 2017
Supervisor: Lillian Røstad, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title: Security Risk Assessment in Software Development Projects

Student: Heidi Svendsen

Problem description:

Software security is increasing in importance. But, a project can usually not spend all their resources on software security. In order to understand what is important to protect in a system, theory says to start by mapping the different risks. Risk assessment will let a project understand the vulnerabilities they face, and prioritise them. When vulnerabilities are prioritised, the project know where to focus their security measures. Risk is the probability of an adverse event happening times the cost of the consequences of that event. Dealing with risk is a continuous task, and will help deal with potential attacks. Risk management does not make the risk go away. It is a way to work with risk analysis over time and to have a complete overview of the potential risks. Risk management includes both risk assessment and risk control.

The thesis will investigate if there is a gap between theory and practise when it comes to risk management and assessments. It will do so by answering the following research questions;

- What is the current state of practice for risk assessment in software projects?
- How does the practice of risk assessment affect software projects?
- What are the benefits and drawbacks of doing risk assessment in software projects in practice?
- What are the differences between software projects using risk assessment and software projects not using risk assessment?

In order to answer these questions both a survey and interviews will be used in software development projects. A self-administrative survey will be sent out before conducting interviews in order to collect background information about the interviewees and their projects. This will also allow for more in-depth interviews with project managers from different interviews.

Responsible professor: Lillian Røstad, IIK

Supervisor: Lillian Røstad, IIK

Abstract

Software security is increasing in importance, linearly with vulnerabilities caused by software flaws. It is not possible to spend all the project's resources on software security. To spend the resources given to security in an effective way, one should know what is most important to protect. By performing a risk analysis the project know which vulnerabilities they face. A risk analysis will prioritise the vulnerabilities, and when the vulnerabilities are prioritised the project know where they should focus their security measures. In software development, risk is usually defined as probability times consequence of an exposed vulnerability. This Master's Thesis investigate the current state of practice for risk assessment in software project. While doing so, it also investigate the effect risk assessments have on software projects and what is perceived as benefits and drawbacks.

During the project a survey were sent out to 200 different organisations, were 21 decided to answer. The survey provided initial data for the current state of practice for risk assessment in software project. At the end of the survey participants could choose to continue to contribute by volunteering to an interview. 8 of the survey participants volunteered to an interview. Results show that 61.9% of the survey participants performed risk assessments for information security in their project. Further, 46.6% reevaluated the risk continuously and the biggest difficulties were lack of time and budget. The interviews resulted in an understanding of the problems organisations face when it come to the risk assessments, such as economical shortcomings. Interviews also showed variation in training of the developers in the projects.

Based on the survey results and the interviews I conclude that it is mostly the larger organisations who perform risk assessments, while the smaller do not want to spend resources on it. Interviews show that the effect of the risk assessment go beyond the software and have a positive effect on the mindset of developers and the culture of the organisation, while the biggest drawback is the economical aspect. Most importantly is the ability to solve problems when they occur, and risk assessment is a great tool for the organisation to be prepared.

Sammendrag

Programvaresikkerhet øker i betydning, lineært med sårbarheter forårsaket av programvarefeil. Det er ikke mulig å bruke alle ressursene til et prosjektet på programvaresikkerhet. For å bruke sikkerhetsressursene på en effektiv måte, bør man vite hva som er viktigst å beskytte. Ved å utføre en risikoanalyse vil prosjektet forstå hvilke sårbarheter de står ovenfor. En risikoanalyse vil prioritere disse sårbarhetene, og når de er prioritert vet prosjektet hvor de skal fokusere sine sikkerhetsresurser. I programvareutvikling er risiko vanligvis definert som sannsynlighet multiplisert med konsekvens som følge av en utsatt sårbarhet. Denne masteroppgaven undersøker nåværende praksis for risikovurdering i programvareprosjekter. Samtidig undersøkes det hvilken effekt risikovurderinger har på programvareprosjekter og hva som oppfattes som fordeler og ulemper.

I løpet av prosjektet ble en undersøkelse sendt ut til 200 forskjellige organisasjoner, hvor 21 bestemte seg for å svare. Undersøkelsen ga grunnleggende data for den nåværende praksis for risikovurdering i programvareprosjekter. På slutten av undersøkelsen kunne deltakerne velge om de ville fortsette å bidra, med et frivillig intervju. 8 av deltakerne i undersøkelsen valgte å delta på et intervju. Resultatene viser at 61,9% av deltakerne gjennomførte risikovurderinger for informasjonssikkerhet i prosjektene sine. Videre gjennomgikk 46,6% risikoen kontinuerlig og de største vanskelighetene var mangel på tid og budsjett. Intervjuene resulterte i forståelse av problemene organisasjonene står overfor når det gjelder risikovurderinger, som for eksempel økonomi. I tillegg viste intervjuene at det er stor variasjon innen sikkerhetskursing av utviklere.

Basert på resultatene fra undersøkelsen og intervjuene konkluderer jeg med at det i hovedsakelig er de større organisasjonene som utfører risikovurderinger, mens de mindre ikke vil bruke ressurser på det. Intervjuene viser at effekten av risikovurderinger ikke bare har en innvirkning på programvaren, men og har en positiv effekt på utviklerne og kulturen i organisasjonen. Den største ulempen av en risikovurdering er det økonomiske aspektet. Likevel er det viktigste evnen til å løse problemer når de oppstår, og risikovurdering er et godt verktøy for organisasjonen til å være forberedt.

Preface

This Master's Thesis is submitted for the degree of Master of Science in Communication Technology at the Norwegian University of Science and Technology (NTNU) in Trondheim, Norway. Research presented in this paper was conducted during the spring of 2017.

Supervisor for this Thesis has been Lillian Røstad, from NTNU's Department of Information Security and Communication Technology. I would like to thank her for help and guidance in this project. Also, this project would not have been possible without the different data received through a survey and interviews. I would therefore use this opportunity to again thank everyone who answered the questions I had, and took time out of their day to help me with this Thesis. Together you have all helped me reach the final results.

Trondheim, June 2017
Heidi Svendsen

Contents

List of Figures

List of Tables

List of Acronyms

BSIMM Building Security in Maturity Model.

CLASP Comprehensive, Lightweight Application Security Process.

EU Eureopean Union.

IRGC The International Risk Governance Council.

NTNU Norwegian University of Science and Technology.

NVD The National Vulnerability Database.

OWASP Open Web Application Security Project.

PCI-DSS Payment Card Industry Data Security Standard.

PII personal identifiable information.

RMF Risk Management Framework.

SAMM Software Assurance Maturity Model.

SDL Security Development Lifecycle.

SSDL secure software development lifecycle.

SSF software security framework.

SSG software security group.

Chapter 1
Introduction

Risk carries many different meanings. For some it carries the expectation of something bad, and for others it carries a thrilling feeling. The International Risk Governance Council (IRGC) defined risk as

> *"an uncertain (generally adverse) consequence of an event or activity with respect to something that humans value. Risks are often accompanied by opportunities."* [IRG08]

This master's thesis will focus on risk associated with software development projects. Every type of project comes with their own value and own kind of risk. In conjunction with software development, the definition from IRGC becomes too broad. Instead, this paper will use the definition given by Barry W. Boehm;

> *"RE = P(UO) * L(UO) where RE is the risk exposure, P(UO) is the probability of an unsatisfactory outcome and L(UO) is the loss to the parties affected if the outcome is unsatisfactory."* [Boe91]

In other words, risk can be defined as probability times consequence. To connect this to the Boehm's definition, consequence is defined as the size of loss or harm to the valued asset [Pel05]. Probability is the statistical chance of a vulnerability in the system being exposed, or the statistical chance of an unsatisfactory outcome. Boehm stated that an unsatisfactory outcome is multidimensional, depending on the stakeholder. Table 1.1 show unsatisfactory outcome based on stakeholders, adapted from [Boe91].

For software development projects it is important to have an understanding of software security to know which software risks the system faces. In his article, McGraw defined software security as *"the idea of engineering software so that it*

Stakeholder	Unsatisfactory outcome
Customers and developers	Overrun in the budget, failure to deliver in time, and schedule slips which cause delays.
Users	Wrong functionality in products, and shortfalls in user-interface, performance, or reliability.
Maintainers	Poor quality software.

Table 1.1: Different definitions on unsatisfactory outcome based on stakeholders, adapted from [Boe91].

continues to function correctly under malicious attack" [McG12]. Software security is a discipline that focuses on both tools, processes, and methods. All this is needed to design, implement, and test software systems. Some basic security goals such as confidentiality, integrity, and availability, together known as the CIA triad [CD05], are important to achieve software security.

Confidentiality: Information that should stay secret, stays secret. Only authorised individuals, entities, or processes may receive access. It may have devastating consequences if unauthorised personnel get access to confidential information. Usually cryptography and access control are used to protect the system's confidentiality.

Integrity: Information cannot be modified by unauthorised individuals, entities, or processes. Nor in an undetected manner. Integrity also concerns trustworthiness, origin, completeness, and correctness of information. Integrity of the source information is an important aspect in software security. Preventive and detective mechanisms are used to protect the system's integrity.

Availability: Information must be readily accessible to authorised users. Usually, business continuity and disaster recovery planning is intended to minimise losses and protect the system's availability.

Other than the CIA triad, accountability, privacy, and non-repudiation are security goals projects should aim to achieve. Accountability means that actions and events can be traced back in time to the user, system, or process that performed the said action or event. This establishes responsibility for actions or omissions. Logs and audit trails are used to protect the system's accountability. If a system does not provide accountability it is not considered secure [CD05]. This is because a system without a safeguard will not be able to learn who is responsible, and what happened in the system. Privacy provide the expectation and right for individuals to privacy

of personal information. Thus the system should handle this information in a secure matter. Personal information refers to information that can identify a human directly, such being for instance a name or an address. Privacy of personal information is in many countries protected by law. This means that organisations are required to protect private data, or they will receive a penalty. Non-repudiation is one of the properties of cryptographic digital signatures. It offers the possibility of proving whether a message has been digitally signed by the holder of a particular digital signature's private key. Non-repudiation is an important, but a controversial subject. It does not provide an absolute guarantee. A digital signature owner may claim that the digital key was stolen, and thus claiming that someone else signed the digital transaction.

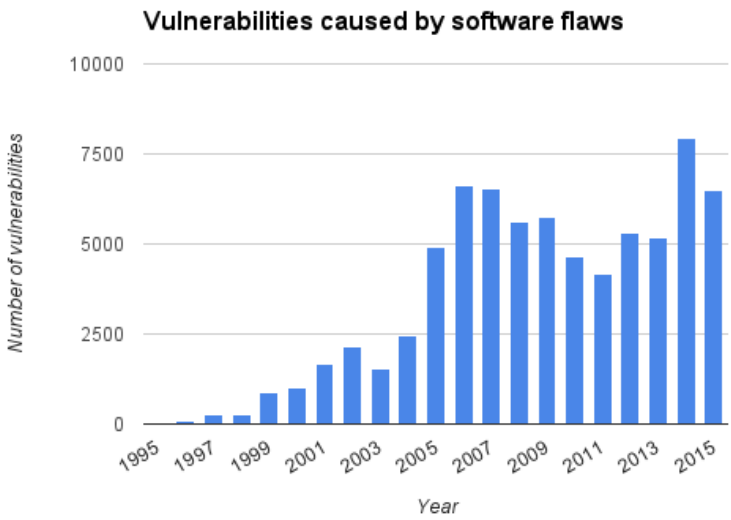

Figure 1.1: Number of vulnerabilities caused by software flaws each year. Data from [NVD].

In the late '90s few people thought much about software security [McG12]. Today it is quite an important part of every software project. The National Vulnerability Database (NVD) includes statistics over vulnerabilities caused by software flaws. Figure 1.1 shows the distribution of vulnerabilities over a 20-year period. Data used to make this graph originated from [NVD]. From the graph, it is easy to see that the number of vulnerabilities have expanded these 20 years. In 1995 there were 25 vulnerabilities. 10 years later, in 2005 there were 4931 vulnerabilities, showing quite an exponential growth. 10 years later, in 2015, there were 6488 vulnerabilities.

Notably, this is over 1500 more vulnerabilities than in 2005. Numbers of software development project have been growing the last years, and will continue to grow in the future. With them, the list of vulnerabilities will continue to grow as well. Because of this, software security is and will continue to be an important part when it comes to software.

Even though software security is an important part of a project, it is not possible to spend all the project's resources on it. Often the project is not about security at all. A lot of systems fail because they protect the wrong things, or they protect the right things the wrong way [And10]. To know what is important to protect in a system, it might be a good idea to spend some time mapping the risk. Handling risk will let the project understand the vulnerabilities they face. By doing a risk analysis a project can prioritise the vulnerabilities [Boe91]. When vulnerabilities are prioritised, the project know where they should focus their security measures. Resources given to software security can then be addressed to the prioritised security parts. Projects with some security measures in place should know what risk they handle. It is also important to understand the risks a project still faces after some security measures are in place [Boe91]. By doing this, a project will be able to make decisions if they can live with the risk not handled. They are also better suited to continue the work on security in the project. Different methods and theories exists on how to identify and handle risk.

One way for handling risk is by risk management. Risk management does not make the risk go away. Risk management is a way to work with risk analysis over time and to have a complete overview of the potential risks. When working with security efforts, it is safe to assume that there should be some kind of risk management included. Included in a good risk management process, is a risk analysis [McG05]. There is the understanding that handling risk should be done in a good matter. This paper will discuss different methods to develop projects securely and methods for risk management in Chapter 2.

Fundamentally, the results for this paper is based on surveys and interviews with project managers from software development projects. The interviews will try to answer if risk analyses and risk management are in use. Both survey and interview are discussed further in Chapter 3. Chapter 4 look into the results retrieved from the survey and interviews, while Chapter 5 will discuss these results.

One of the goals for this paper is to discuss if theory transfers to practice when it comes to risk handling and management. It will discuss if risk analyses work, and how the experience of using it is. One assumption is that there exists a gap between theory and practice. If there are cases where risk analysis and risk management are not in use, it is discussed why not.

Chapter 2
Background

Regardless of the design and implementation, attacks will happen [McG12]. Because of this, it is important to monitor the system. But a good monitoring mechanism will not make up for poor security implementations. One of the major challenge of software is to create it secure and in need of less updates through patches [LH05].

Boehm [Boe91] stated that identifying risks early in the development would help lessen long-term costs. It could also help prevent software disasters. Risk handling is a continuous task, and when done correct, it will help deal with potential attacks. Risk management is a great tool to work with risks over the project period. Presented in this paper are two different processes for risk management, Boehm's risk management process and the risk management framework. Both these processes explain risk management at a higher level, giving a great understanding of steps that should be included in a risk management process. These two processes are not developed into the development process, but rather next to it. This means that it might be harder to implement as the development process progresses. It might be hard to know when to perform the different steps, or when to revise some steps. But, since they are next to the development process, they can be implemented independently of the chosen development process. This means that both the risk management possesses can be used in any development process.

Even knowing a risk management processes such as Boehm's risk management process or the risk management framework, it might be hard to know what to look for and where to start. Building Security in Maturity Model (BSIMM) is a model that describes how the state of software security is at the moment of the study. This type of model is called a descriptive model. Descriptive models can be used to determine how a company is doing compared to others. This paper will take a closer look at BSIMM, in order to investigate activities most in use. BSIMM can help in the risk management process by explaining security measures 95 other organisations have. From this the organisation can find the security measures most interesting for them.

In addition to descriptive models, there are prescriptive models. Prescriptive models are models that describes what one should do. Prescriptive models mentioned in this paper are Software Assurance Maturity Model (SAMM), Microsoft Security Development Lifecycle (SDL), SDL-Agile and the cigital touchpoints. SAMM, as BSIMM is a maturity model, and both are composed of 12 practises. SAMM explains how an organisation can achieve a maturity level, and can be used to measure progress in the security aspects.

Risk management processes may face the problem that they are executed next to the development process, not integrated in it. By integrating risk analysis into the development process, and including the developers, the understanding of risk will become greater. Microsoft have created secure lifecycles for development processes, Microsoft SDL and SDL-Agile. SDL-Agile is designed to specially fit agile teams and agile development. Different from BSIMM and SAMM, Microsoft SDL and SDL-Agile give an explanation of when the different development steps should be executed. Both Microsoft SDL and SDL-Agile include some aspects collected from the risk management process, for instance threat modelling.

Using neither Microsoft SDL nor SDL-Agile, an organisation can develop their own lifecycle. This might be more suited for their products. The cigital touchpoints are meant to be applied throughout a lifecycle, because they are a basis for best practises in software security. Included in the touchpoints are both risk analysis and risk-based security tests, and it is illustrated where in the lifecycle they should be executed.

2.1 Risk Management

An important part in dealing with risk is the method of risk management. Two different methods are presented in this Chapter. One is Boehm's risk management process, presented in his paper *"Software risk management: principles and practices"* [Boe91]. This article was published in 1991, but it is still relevant when it comes to the risk management process. The other method, Risk Management Framework (RMF) is presented in the book *"Software security: building security in"* [McG06], and in the article *"Risk Management Framework (RMF)"* [McG05] both by Gary McGraw. Both Boehm's risk management process and RMF explain risk management at a higher level, giving a great understanding of steps that should be included in a risk management process.

2.1.1 Boehm's Risk Management Process

Both Boehm [Boe91] and Khan, Khan, and Sadiq [KKS12] recommend a model of different steps included in risk management, illustrated in Figure 2.1. Per this model,

risk management involves two initial steps, risk assessment and risk control. Under these two initial steps are there for each, three subsidiary steps.

Under the risk assessment step are the subsidiary steps risk identification, risk analysis, and risk prioritisation. Risk identification lists the risks that can compromise the success of a project. Boehm suggest using checklists, analysis of assumptions, and decision-driver, in addition to decomposition, as techniques for risk identification. Next subsidiary step, risk analysis, assess the probability and size of the loss of identified risk items. A risk analysis also assess combined risk in risk-item interactions. Models for performance and cost are two techniques for risk analysis. Other techniques include analysis of network, decision, and quality. Risk prioritising ranks and orders the identified and analysed risks. Techniques for risk prioritising include reduction of compound-risk, as well as analysis of risk exposure and risk leverage.

Under the risk control step are the subsidiary steps risk management planning, risk resolution, and risk monitoring. Risk management planning help coordinate plans for the identified risks. The step also includes making a project plan. For risk management planning techniques, Boehm suggest to use checklists of risk resolution techniques, analyses of what benefits the cost, and standard risk management plans. Next subsidiary step, risk resolution, eliminates or resolves risk items. Simulations, use of prototypes, and benchmarking are some of the techniques suggested, in addition to analyses of missions and have key personnel agreements. Risk monitoring tracks the progress of resolving risk items. Techniques for risk monitoring includes tracking milestones and a top 10 risk item list, reassess the risks, and take corrective actions.

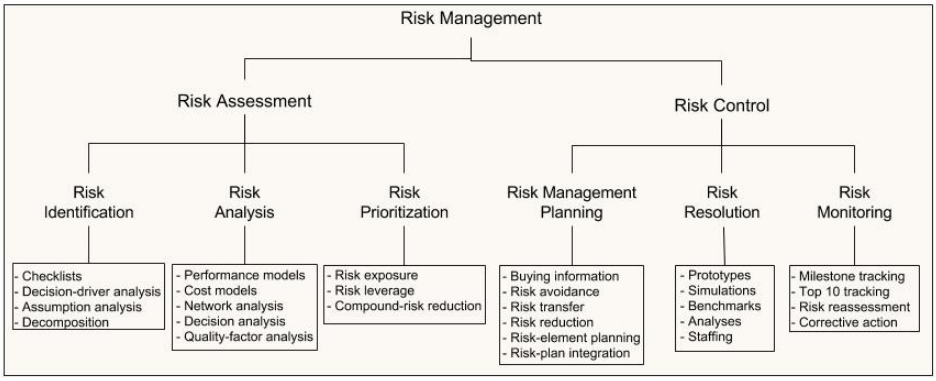

Figure 2.1: Boehm's risk management process

Boehm [Boe91] investigated risk management in projects and found that the successful project managers generally were good risk managers as well. They used general

concepts of risk exposure, and not terms as risk identification, risk assessment, risk management planning or risk monitoring. From his investigations Boehm made a top 10 list over the primary sources of risks in software projects. Table 2.1 show this list, and is based on a survey of several project managers.

Risk item	Risk-management technique
Personnel shortfalls	Having a staff consisting of top talent, build teams, hold cross training and have key personnel agreements.
Unrealistic schedules and budgets	Use a detailed estimate of cost and schedule from multiple sources, reuse software, increment the development, and scrub the requirements.
Developing the wrong functions and properties	Analyse both the organisation, the mission, off-nominal performance and quality-factors, conduct user surveys and participation, and prototyping.
Developing the wrong user interface	Conduct user participation, analyse tasks, prototyping, and plan for different scenarios.
Gold-planting	Scrub the requirements, analyse what benefits the cost, and prototyping.
Continuing stream of requirements changes	Hold the threshold for change high, and increment the development.
Shortfalls in externally furnished components	Use inspections and benchmarking, check the references, and analyse the compatibility.
Shortfalls in externally performed tasks	Check the references, use preaward audits and award-fee contracts, and have competitive design and prototyping.
Real-time performance shortfalls	Use prototyping, benchmarking, simulations, instrumentation, and modeling.
Straining computer-science capabilities	Analyse what benefits the cost and the technical, check reference, and use prototyping.

Table 2.1: Top 10 list over the primary sources of risks in software projects according to the article of Boehm

Implementing a risk management process is easy and inexpensive. Boehms process provides improvements early in the lifecycle, and it contains familiar parts from other risk management practises. This is helpful for managers already familiar with one risk management practice. However, this is not a cookbook approach. To handle

all the people-oriented and technological-driven success factors in a project, it is necessary to have good measure of human judgement as well as the technology skills [Boe91]. As for other projects, a project with a risk management process include a great measure of human judgement. Most important for risk management is to get a good measure of the project's critical success factors.

2.1.2 Risk Management Framework

Gary McGraw suggested RMF as a framework for risk management. The key to RMF is to find and keep track of risks as the project progress. It has some similarities to Boehm's risk management process, but RMF focuses much more on linking the different risks to a business context. If a technical risk is connected to a business aspect it is easier to convince non technical personnel why it is important to look at the risks a system is facing. Essentially, RMF work as an approach to security work and it is designed to manage software induced business risk. It might be integrated in a secure software development lifecycle (SSDL). The framework consist of five different activities, as shown in Figure 2.2 [McG05]. The five activities consist of [McG05];

Understand the business context: This activity consist of understanding how management of risk is impacted by business motivation. It is important to get a handle on the business situation. An analyst need to describe the different business goals, priorities, and circumstances. This is important in order to understand which software risks to care about.

Identify and link the business and technical risks: This activity consist of identifying both business risks and technical risks, and linking them together with the business goals. In this stage it is important to describe the risks carefully in order to mitigate them in a smart way.

Synthesize & rank the risks: This activity consist of prioritising the risks identified in the previous step. It is important to figure out what to do first in the current situation and how to allocate resources. Prioritisation must take into account the business goals that are most important to the organisation, which goals are immediately threatened, and how likely the risks are to manifest.

Define the risk mitigation strategy: This activity consist of creating a strategy to mitigate the prioritised risks in the most cost efficient manner. Strategies are constrained by the business context, and should always consider the organisations cost. It is important to have a validation plan as well, to show that the risks have indeed been mitigated.

Carry out fixes and validate: This activity consist of the actual mitigation. It is important to follow the strategy formed in step four, in order to spend the

resources in the best possible way. The validation of the mitigation also happen in this activity to provide some confidence that the mitigation worked.

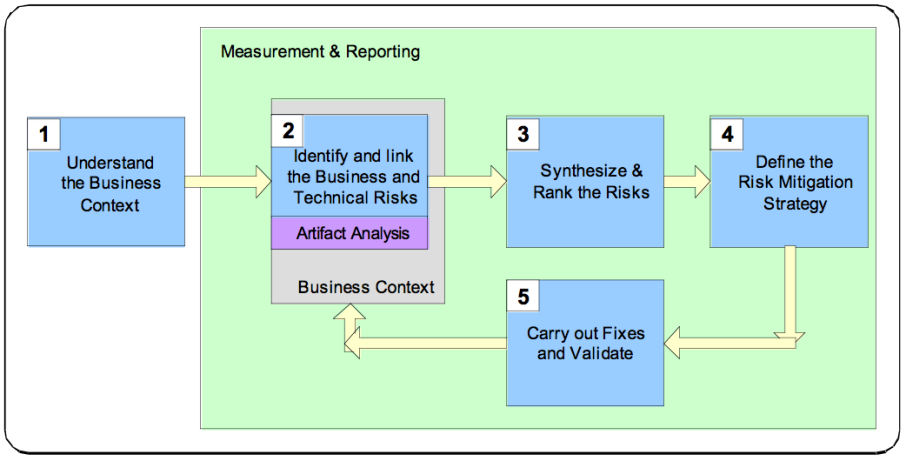

Figure 2.2: Illustration of the Risk Management Framework

What characterises a successful use of RMF, is continuous and consistent identification and storage of risks. This means that identifying risks only once is not sufficient. A list over risks should be maintained at all times, and continually be revisited. Figure 2.2 shows the lifecycle in a particular order, but the activities may need to be applied multiple times through the project. Then the particular ordering may be applied in many different ways.

2.2 Building Security in Maturity Model

BSIMM is an observed-based study, it describes the common ground of software security shared by 95 different companies. It is a descriptive model, meaning that it describes how the state of software security actually is in these 95 companies. The work on BSIMM started in 2008, and the latest study, BSIMM 7 [MMW16], was published in 2016. BSIMM is organised as 113 different activities. These activities are categorised in a software security framework (SSF) composed of 12 practises in four domains, shown in Table 2.2.

Governance includes practises that help organise, manage and measure an initiative. Also central in the governance practice is the development of the staff. Most used activity in this domain is the compliance and policy activity 1.2 – Identify PII

Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy & Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance & Policy	Security Features & Design	Code Review	Software Environment
Training	Standards & Requirements	Security Testing	Configuration Management & Vulnerability Management

Table 2.2: The SSF of BSIMM, consisting of 12 practises in four different domains.

obligations. The software security group (SSG) identify and describe the personal identifiable information (PII) obligations, both from the regulations and customers expectations. This information is used to promote best practises for privacy.

Intelligence includes practises that result in collections of corporate knowledge used in carrying out software security activities throughout the organisation. Collections include both proactive security guidance and organisational threat modelling. Most used activity in this domain is the security feature and design activity 1.1 – Build and publish security features. Instead of having each team implement their own security features, SSG should provide proactive guidance. SSG can build and publish security features for other teams to use, a method to better the security in the organisation. Teams benefit from these pre-approved implementations, and the SSG does not have to track down errors in the security features made by different teams.

SSDL Touchpoints includes practises associated with analysis and assurance of particular software development artefacts and processes. All software security methodologies include these practises. Most used activity in this domain is the architecture analysis activity 1.1 – Perform security feature review. Reviewers who are security-aware will identify security features in an application, and then study the design to look for problems causing these features to fail or prove insufficient.

Deployment includes practises that interface with traditional network security and software maintenance organisations. Software configuration, maintenance, and other environment issues have direct impact on software security. Most used activity in this domain is the configuration management and vulnerability management 1.2 – Identify software defects found in operations monitoring and feed them back to development. Content of logs can be revealing, or reveal the need to improve the log. Ideally, feeding the defects back to development it will close the information loop

and make sure the problems get fixed.

Using the 113 activities, BSIMM studies which of them are in use in the companies they studied. The most used activities listed in the four domains are four of the 12 activities that ”everybody” use [MMW16]. Still BSIMM explain that they cannot directly conclude that these activities are necessary for all software security initiatives. They only say that these are commonly found in highly successful programs.

To determine how one company stands relative to others, the model can be used as a measuring stick. First step is to identify the activities existing in the project. Then start implementing the ones that are missing and needed. It is important to notice that a company should not try to start on the third level. They should rather focus on the first level and move on when this level is truly embedded [Jaa12]. BSIMM reflects the current state in software security. It is neither a ”how to” guide or a one-size-fits-all solution. BSIMM aim to help software security communities. They help companies with planning, carrying out, and measuring initiatives on their own.

2.3 Software Assurance Maturity Model

SAMM [Cha09] is a framework to help organisations plan and implement a software security strategy tailored to the specific risks facing the organisation. As BSIMM, SAMM is a maturity model. The difference between the two models are that SAMM is a prescriptive model, while BSIMM is a descriptive model. A prescriptive model is a model that describes what should be done. SAMM is composed of 12 security practises, in four different business functions, as shown in Table 2.3.

Governance	Construction	Verification	Deployment
Strategy & Metrics	Threat Assessment	Design review	Vulnerability Management
Policy & Compliance	Security Requirements & Design	Code Review	Environment Hardening
Education & Guidance	Secure Architecture	Security Testing	Operational Enablement

Table 2.3: The structure of SAMM, consisting of 12 security practises in four business functions.

The business functions are related to different aspects of software development. All organisations need to fulfil each of these business functions to some degree. The four functions are [Cha09];

Governance: Processes and activities related to how an organisation manages overall software development activities. This includes concerns that cross-cut groups involved in development as well as business processes that are established at the organisation level.

Construction: Processes and activities related to how an organisation defines goals and creates software within development projects. In general, this will include product management, requirements gathering, high-level architecture specification, detailed design, and implementation.

Verification: Processes and activities related to how an organisation checks and tests artifacts produced throughout software development. This typically includes quality assurance work such as testing, but it can also include other review and evaluation activities.

Deployment: Processes and activities related to how an organisation manages release of software that has been created. This can involve shipping products to end users, deploying products to internal or external hosts, and normal operations of software in the runtime environment

Each business function define three security practises. Each practice contains an area of security related activities, which build assurance for the related function. This means that there are 12 security practises independent from each other, which improve the understanding of the business functions. The security practises again exists of three maturity levels, objectives. In order to reach one objective, activities included in the maturity level should be completed.

All the critical business functions take part in the model. SAMM aim to aid organisations in evaluating the existing software, building a balanced software security assurance program, demonstrating concrete improvements and measuring security-related activities. SAMM offers good tools for self-assessment and planning. It is now managed by the Open Web Application Security Project (OWASP), and is therefore freely available for all to use.

2.4 Security Development Lifecycle

SDL is a process developed by Microsoft. They integrated their collected experience in software security into this process. The work on SDL started in 2002. Different development groups from Microsoft wanted to find ways to improve the existing security code [Micb]. Core aspect of this process is to develop an understanding of the risks a system faces [Pot09]. SDL let different projects add security related steps in development, testing and releasing. The different steps are shown in Figure 2.3 [Micc], and this process is used to identify vulnerabilities and determine a way to

address them. SDL consists of the core steps [Micc] – Training, Requirements, Design, Implementation, Verification, Release, and Response.

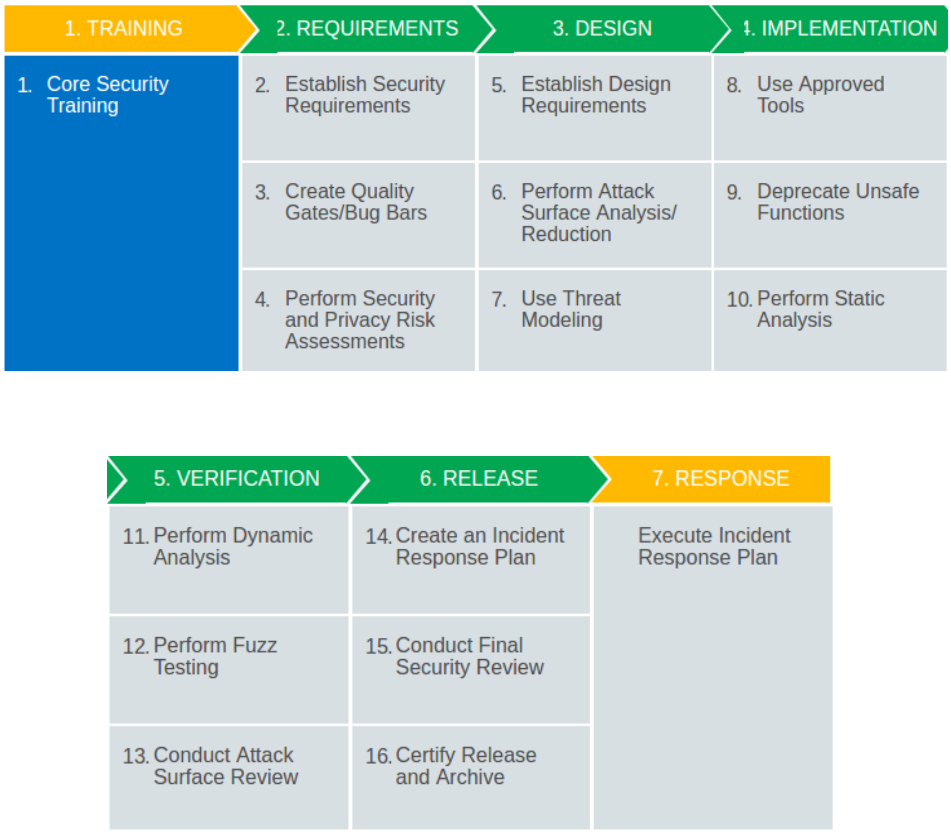

Figure 2.3: Illustration of SDL processes

Training is a commitment to understand security basics and keep up with the latest developments in security and privacy. This can be done with core security training, and parallel with the requirement and design step. Requirements is the step that consider foundational security and privacy issues. This step analyse quality and regulatory requirements in consideration to cost and business needs. One of the activities in this step is SDL practice #4 – perform security and privacy risk assessments, one example where SDL include risk analysis in the lifecycle. Practice #4 involves examining software design to help teams identify what part of the project requires threat modelling and security design reviews. Examinations are based on cost and regulatory requirements. Practice #4 also tries to determine a privacy impact rating for features, products or services.

The design step will establish best practises for design and functional specification. Risk analysis are performed to help mitigate security and privacy issues. In the design step SDL practice #7 – use threat modelling, is performed. Threat modelling consist of modelling different scenarios to expose different threats and establish mitigations. Threat modelling is explained in more detail in Section 2.4.1. Implementation is a step to help the end user to make informed decisions about secure ways to deploy the software. It includes establishing practises to detect and remove security issues from the code.

Verification will ensure that the code meet the security and privacy requirements established in the previous phases. SDL practice #13 – conduct attack surface review, help ensure that possible design or implementation changes have been taken into account. New attack surfaces created have to be reviewed and mitigated in the threat model. Release includes making a project ready for public release, and making a plan how to effectively perform updates, both for servicing tasks, and to address security and privacy vulnerabilities that may occur. The response step makes an organisation able and available to respond to any reports of emerging threats and vulnerabilities. If needed there exists response plans that can be executed in this step.

SDL involves modifying the development process by integrating the measures that lead to improved software security [LH05]. Microsoft believes that software can be created to defend itself from attackers. Developers must understand where the threats are realised and how the software addresses them [Pot09]. According to Microsoft [Mica] SDL aims to improve both productivity, application security, and productivity. SDL goes beyond the compliance requirements of today, enabling an organisation to take a proactive and a forward-thinking approach.

2.4.1 SDL Threat Modelling

Threat modelling allows software architects to both identify and mitigate potential risks early in the process. As Boehm [Boe91] stated, identifying risks early in the development would help lessen long-term costs, therefore threat modelling will help reduce cost. In Microsoft SDL, threat modelling is included in the design step of the lifecycle.

Microsoft have their own threat modelling tool proposed for SDL, the SDL Threat Modelling tool [Micg]. This tool is not just designed for security expert, but is easy to use for all developers. Unlike other threat models, the SDL threat model is centred around the software, and not assets or attackers. It builds on familiar activities, such as drawing pictures of the software architecture. Microsoft SDL approaches threat modelling with a focus on design analysis techniques. The process of the SDL threat model is shown in Figure 2.4. With a vision for the feature or product the developer or architect make a diagram of it. Thereafter potential threats are identified before

a mitigation plan is suggested. To know if the mitigation plan work, it is put into work and then validated. When new attack surfaces are introduced they are entered into the diagram, threats are identified and mitigated, before the feature or product is validated again. SDL threat modelling is making threat modelling a part of the development process.

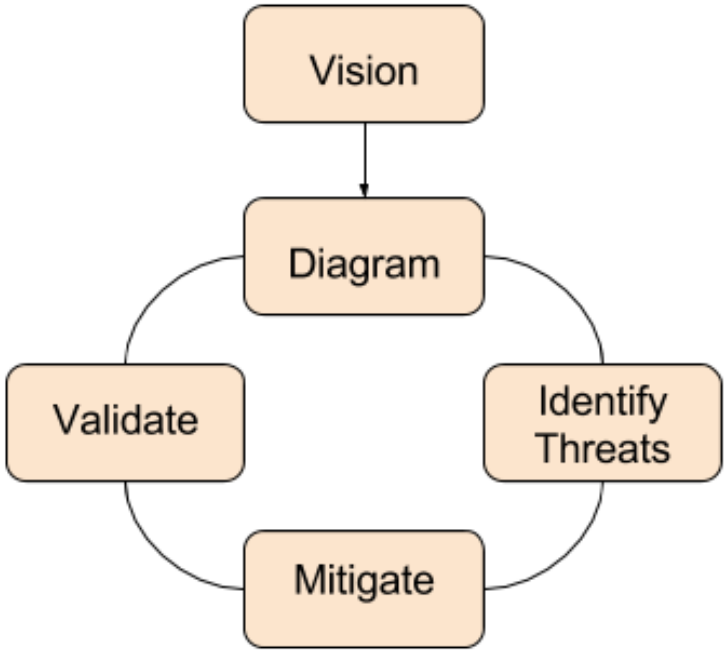

Figure 2.4: Illustration of SDL Threat Modelling processes

2.5 Security Development Lifecycle - Agile

The development and management method agile has become more popular to use than the classic waterfall method. Microsoft says [Mice] that security is not given enough attention with the agile method, because the focus lays on rapid creations to satisfy the customers direct needs. Therefore Microsoft developed SDL into a tailored agile-development framework called SDL-Agile. This process was made to integrate security practises into the agile method. For this process, the security practises are reorganised into three categories [Micf] – Every-Sprint practises, Bucket practises, and One-Time practises. These three categories are illustrated in Figure 2.5, Figure 2.6, and Figure 2.7, respectively. All three figures are from [Micd].

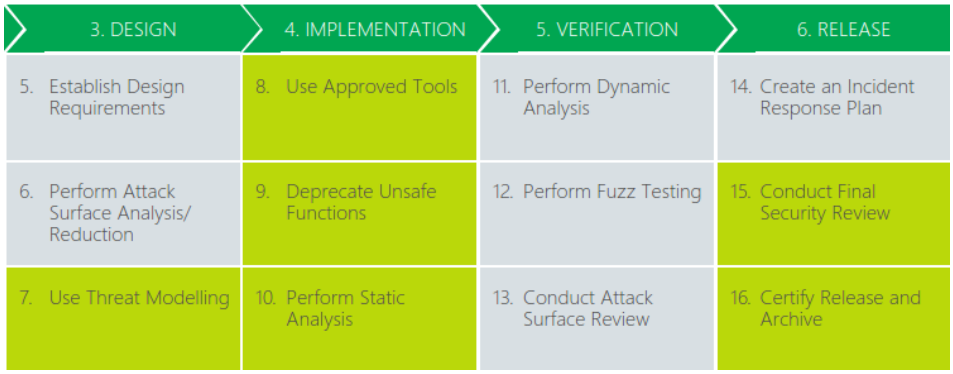

Figure 2.5: SDL requirements included in the Every-Sprint practises is in this figure illustrated in light green.

A sprint is a short period of time, usually 15 to 60 days. SDL-Agile projects is built up by a few of these sprints. A project will have a product backlog which includes a list of features to be added in the product. Prior to each sprint some of these features are selected and added to the sprint backlog [Micf]. These tasks are then to be completed in the assigned sprint with respect to the different requirements in the categories described above.

Every-Sprint practises exists of SDL requirement so essential to security that no software should be released without these being met. It does not matter how long each sprint is, all requirements in this category must be completed in each sprint or the sprints is incomplete. Figure 2.5 illustrates the requirements included in Every-Sprint practices, highlighted in light green. One of the requirements included in the every-sprint practises is SDL practice #7 – Use threat modelling [Micd]. Threat modelling is a risk management tool that have been implemented in the Microsoft SDL and SDL-agile. This tool is considered to be so essential that it should be included in each sprint. It is included because each sprint will bring new attack surfaces and new risks to consider. Threat modelling is explained in more detail in Section 2.4.1.

Bucket practises consists of tasks that must be performed on a regular basis over the lifetime of the project. They are not so critical that they need to be performed for each sprint. The category is divided into separate buckets of related tasks – verification, design review, and planning. Figure 2.6 illustrates the requirements included in Bucket practices, highlighted in light green. Product teams complete one requirement from each bucket during each sprint. Risk analysis can in bucket practises be seen as SDL practice #13 – conduct attack surface review. This practice help ensure that possible design or implementation changes have been taken into

account. New attack surfaces created have to be reviewed and mitigated in the threat model.

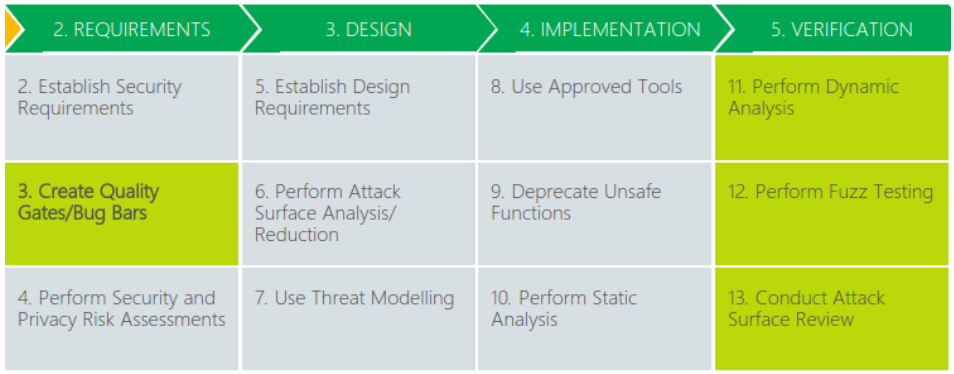

Figure 2.6: SDL requirements included in the Bucket practises is in this figure illustrated in light green.

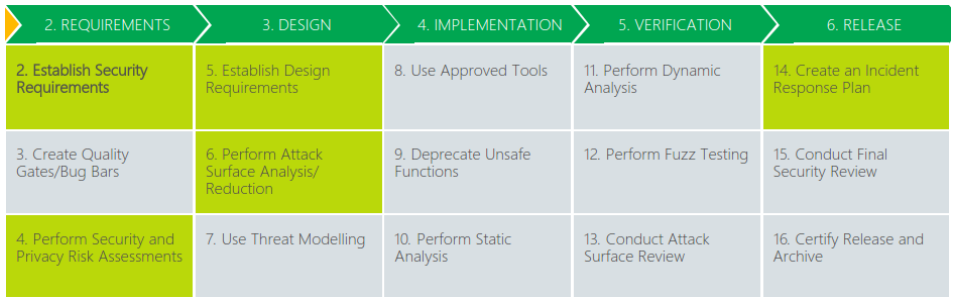

Figure 2.7: SDL requirements included in the One-Time practises is in this figure illustrated in light green.

One-Time practises includes tasks that need to be met at the start of a project, these usually do not need to be repeated after they are completed. Generally these tasks are easy and quick to complete, but when completing the rest of the sprint requirements it is not feasible to complete the one-time requirements in one sprint. Figure 2.7 illustrates the requirements included in One-Time practices, highlighted in light green. SDL-Agile allows a grace period to complete each one-time requirement, this period ranging from one month to one year after the project start. One of the requirements included in one-time practises is SDL practice #4 – Perform security and privacy risk assessments [Micd]. Practice #4 show an example where risk assessments are implemented in the SDL-Agile process. An incident response plan is also a tool for risk management. It includes helping to prepare for new threats that emerge.

In addition, the developers and the security experts have a plan for how to handle attacks.

2.6 Cigital Touchpoints

Gary McGraw described in his book *"Software Security: Building Security in"* [McG06] seven touchpoints for the best practises of software security. The touchpoints are meant to be applied throughout the software lifecycle, because the basis for the best practice is both good software engineering and explicitly evaluating the security situation. Knowledge and understanding of common risks, designs for security, risk analysis and testing is the basis of the touchpoints. Figure 2.8 [McG06] illustrate in which software artifact McGraw believed his touchpoints should be executed.

"To attain software security, software projects must apply the touchpoints throughout the software lifecycle, practicing security assurance as they go." [McG06] Gary McGraw wrote in his book.

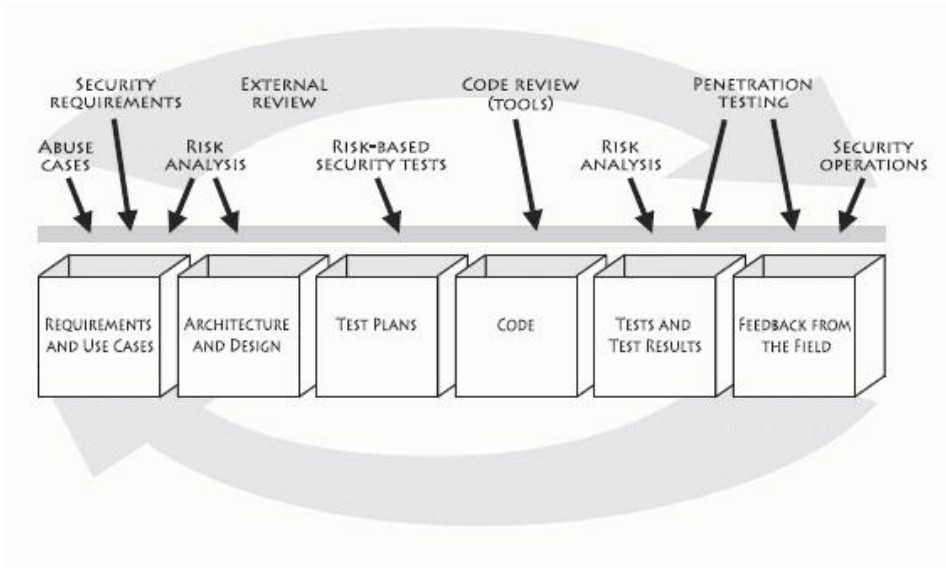

Figure 2.8: The Cigital Touchpoints. Best practises of software security, shown by arrows, are applied to various software artifacts, shown by boxes.

Although Figure 2.8 seems to follow the traditional waterfall model, the touchpoints will be cycled through more than once to follow a more iterative development approach. The illustration does not necessarily show in which order the touchpoints are most efficient. McGraw came up with a list of the touchpoints, ordered by their effectiveness on software security [McG06];

Code review: Here the focus lay on the implemented bugs. By using static analysis tools these bugs and other vulnerabilities can be discovered. But, code review is not a sufficient practice for achieving secure software.

Architectural risk analysis: Here the security analyst will uncover and rank architectural flaws in order to start mitigating. Architectural risk analysis is necessary at both the specification-based architecture and the class-hierarchy design stage.

Penetration testing: Understanding the software in its real environment. If the software passes the penetration test, it says little about the security in the system. Passing a penetration test is not equivalent to having no vulnerabilities. On the other hand, if the system fail the test this indicates that the software have some flaws.

Risk-based security tests: Here security tests are done on the system. Included in this stage both testing of security functionality with standard functional testing techniques and risk-based security testing based on attack patterns, risk analysis results and abuse cases should be included.

Abuse cases: Here the system's behaviour is described when under attack. It is similar to use cases, but to build an abuse case it requires coverage of what should be protected, both from whom and for how long. This is a great way to enter the mind of an attacker.

Security requirements: Here security requirements are identified and maintained. This is a complex job which deserves a lot of attention. Good requirements should cover both functional security and emergent characteristics.

Security operations: Here network security professionals are encouraged and allowed to get involved with applying the touchpoints. They provide experience and security wisdom to the development team. Attacks will happen regardless of the strength of the system, and it is therefore important to understand the software behaviour and monitor it. Knowledge learnt here should be cycled back into the development.

Importance of risk management is acknowledged by the touchpoints [DWSB+09]. Cigital touchpoints include theory from risk management, such as the touchpoints architectural risk analysis, and abuse cases. Architectural risk analysis are suggested to be performed when finding requirements and use cases, when deciding architecture and design, and when doing tests. This touchpoint will help find the impact of different risks, and show the importance of mitigating them. Threat modelling is seen in the cigital touchpoints as well as in Microsoft SDL and SDL-agile. The touchpoint is called abuse cases and is threat modelling based on the method of use cases.

Chapter 3
Methodology

Analysing a finished product will only show the state that the security is in at that particular moment. How the process was conducted to get this state will not show in a launched product. Therefore, it is not possible to say anything about risk management by only looking at the final product. Looking at different stages of the product will also not reveal the risk process, but it will show if the developers worked on security during the development lifecycle. In order to answer the research questions for this paper, the methods used will be a self-administrative survey and interviews.

A survey is used to gather information for statistical models. The survey will contain questions about the type of team, their basic knowledge about information security and risk management, and how the projects security and risk management processes are. Appendix A provides the survey that was sent out to the organisations. While the survey give an understanding about the market, in-depth interviews allow for a deeper understanding. An interview will allow to question why a specific model is used, or why none of the risk management processes are in use. Interviewing different project managers will open up the possibility to question the team's knowledge about security and software risks.

Both a survey and an interview consist of information gathering from people and their software project. This raises some ethical concerns the researcher should be aware of. Silverman lists some of the general principles for ethical research in his book *"Doing Qualitative Research"* [Sil09]. In this list he includes that the researcher should protect the research participants, get informed consent, and open for the possibility to withdraw this consent at any moment. Research come with both benefits and risk, the assessment of them should be clear to the participants. Silverman conclude the list by mentioning that a researcher should not do any harm to the research participants and their work.

This study will include anonymous research participants. No information about who they are, their workplace, or their projects will be published. Answers to either the survey or an interview will not be traceable to the connecting project, person or company. Together with the survey, a consent form, and information about this project were sent to different companies. At the end of the survey, the participants were asked if they were willing to participate in an interview as well. Hence it was possible to contribute through the survey only, or through the combination of the survey and an in-depth interview.

3.1 Survey

Fowler wrote a book called *"Survey Research Methods"* [FJ13], about standard and practical method designed to provide statistical descriptions. In his book a survey is characterised as a method to produce a quantitative, or numerical, description of the studied population. The main way of producing this statistic is to ask questions to the studied population. Rather than question every single member of the population, only a fraction of the population is used to gather information. A survey is a comprehensive method to collect information. This information will be used to describe, compare, or explain both knowledge, attitudes, and behaviour. A survey can be conducted in many different ways – as a questionnaire completed by the subject, as a telephone survey, as an interview, or by observing participants behaviour. The method used for this project will be a questionnaire completed by the subjects, and later semi-structured interviews. Interview as a method is explained more in Section 3.2.

According to Kitchenham and Pfleeger [KP08] there exists two common designs for a survey – longitudinal and cross section. Longitudinal study collect information about changes in a population. Changes happen over a specified time period, the study either question the same people at different times, or question different people at different times. A longitudinal study is therefore a forward-looking study. Cross section survey collect information about a topic at one point in time. Different people are questioned at the same, specific time. A cross section survey retrieve information as a snapshot of what is going on in the studied population. Kitchenham and Pfleeger have only cross section surveys as examples, according to them this was not a coincidence. In their experience most surveys in software engineering are cross section studies.

The design of the survey questions is important. Questions should be designed such that they can produce statistical data. Kitchenham and Pfleeger [KP08] recommend to design questions with answers in one of the following four categories;

1. Numerical values
2. Response categories
3. Yes/No answers
4. Ordinal scales

Numerical values are usually straightforward, examples are questions about age, whole hours, and the size of a team. Response categories require the participant to choose from a set of pre-decided answers, examples are job type, resident country, and studies known to the respondent. The set of pre-decided answers should not be too long, but still exhaustive, mutually exclusive, and allow for multiple selection. Yes/No lack reliability because the respondent do not give the same answer at different times. Still, this type of answer will allow to make statistics and to divide the answers into categories. Last category is ordinal scales, which will allow for attitudes and preferences, some examples are agreement scales (e.g from strongly disagree to strongly agree), frequency scales (e.g. from never to most of the time), and evaluation scales (e.g. from terrible to excellent). The question category ordinal scales was not used in the survey for this project. In all of these categories the researcher should figure out if it is appropriate to include a ”Do not know” or ”Not relevant” answer. Participants may use this alternative to avoid the question, however the answers will then not be forced and the answers might contribute more to the research.

Many times a written answer is used in addition to the categories listed above. This category let the respondent give their opinion freely in a written form instead of only answering with pre-decided answers. Questions still need to produce a statistical result, and therefore the researcher should be aware that the form of written answers are harder to process. They can be used to quote the participants, and to comment on the results. This was the purpose for texts answers in this survey.

3.1.1 Survey as a Method

The survey used in this project was a self-administrative questionnaire. This means that the respondent of the questionnaire had to understand the questions without any other information than the survey. The questionnaire was distributed by e-mail to the participants, together with the consent form and information about the project. By answering the survey the participants approved of the consent form, as they were informed about this beforehand of the survey. The survey asked questions about risk analysis and management for a fixed project, therefore the questions were about a fixed time in the participants projects, meaning the survey was a cross section survey.

When considering the design of the questions, this questionnaire used both Numerical, Response categories, Yes/No, and a few written answers questions. Numerical questions were used to learn how many had knowledge of security in the team, or how much of the resources are used on security for a team. An example from the survey is question 3, "How many are working in your team?". Yes/No answers were used to learn if someone in the team had worked with security before, or if the project needed security. An example from the survey is question 25, "Have there been performed risk assessments for information security in the project?". Written answers were used to learn the role the participant had in the team, and how risk is managed at the moment the survey were filled. An example from the survey is question 20,"How is risk handled in the project at this time?".

The category used most often in this projects questionnaire was the response category. These questions had some pre-decided answers, and most of them had an "other" answer as well. The "other" answer let the participant fill in an answer if it was missing in the pre-decided answers. One example is question 10. "In what industry will the end product be in use?", which had eight different answers – finance, commodity, production, telecommunications, technology, energy, transport and logistics, and medicine – as well as the "other" choice. The full questionnaire is found in Appendix A, it is in Norwegian as this was the language it was distributed in.

A survey will try to answer the research questions "What is the current state of practice for risk assessment in software projects?" and "What are the differences between software projects using risk assessment and software projects not using risk assessment?". The survey was chosen as a method because of its advantage in retrieving statistical answers. Ideally, the survey will provide statistical data to answer these two questions.

3.1.2 Aspects That May Introduce Inaccuracies

The researcher should be aware of the different pitfalls that comes with a survey. Since the participant answer the questions by himself, the wording need to be easy and understandable. If the questions are unclear, the answer might not be correct or the participant may choose not to answer the question. There is also the possibility of making the participant feel like the questionnaire is to hard, and therefore choose not to finish the questionnaire in its entirety. In the survey for this project only question 25, "Have there been performed risk assessments for information security in the project?", was mandatory to answer. This means that any participant can choose not to answer questions he find too hard, or do not know the answer to.

For survey as a method, it is not only the wording of the questions that may cause errors. The length of the individual questions, as well as the length of the questionnaire itself may cause errors in the results. If the individual questions are

too long or, they might be harder to understand and therefore the participant may not catch the correct meaning of the question. If the entire questionnaire is too long, the participants may get bored or simply decide he do not have the time to complete it. This may result in a participant that rushes through the last part of the survey, not giving the questions enough thought. Or the participant may just quit the survey all together. The survey for this project takes five to ten minutes to complete.

3.2 Interview

According to Myers and Newman [MN07], interview is one of the most important data gathering tool for qualitative research, and also the most common. Qualitative studies are studies that include details from participants', in addition to their motivations and intentions. Interviews allow the researcher to view and examine information not ordinarily shown. They are used to describe a person's life *"as lived, felt, undergone, made sense of, and accomplished by human beings"* [Sch07]. A person's worldview is mostly invisible to others, because experiences are in depth different from one person to another [SA11]. Thus a researcher have to try to understand the world from the interviewee's perspective to unfold the meaning of the interview, the researcher is engaged in the production of data.

It exists a number of different types of qualitative interviews. Three of them are structured interview, unstructured or semi-structured interview, and group interview [MN07].

Structured interview: In this type of interview it exist a complete script prepared beforehand. The researcher follows the script with no room for improvisation. This type is most used where interviews not necessarily are conducted by the researcher.

Unstructured or semi-structured interview: In this type of interview it exist an incomplete script. The researcher follows the prepared script, but have to improvise where the script is incomplete.

Group interview: In this type of interview two or more people are interviewed at the same time. A group interview can be either structured or unstructured.

Qualitative research in information system typically use unstructured or semi-structured interviews. A semi-structured interview allows the researcher to create a space where the participant can reveal their personality and identity. For this to happen it is important that the researcher show empathy, understanding, respect, and interest towards the interviewee. Interviews are regarded as a socially and linguistically complex interaction between people. It involves active listening

and engagement from the researcher. According to Schultze and Avital [SA11], the interview is seen as a way to construct meaning and not to collect facts.

3.2.1 Interview as a Method

Interview is a method where at least two people, one being the researcher, exchange views on a common interest. The interview is the best method to understand how risk analysis and management are used in real-life projects. As a social interaction, the interview is a great tool to now learn first-hand how risk is handled. But the interview itself will not guarantee production of meaningful and rich data. In order to generate rich data, the interview have to include some method characteristics according to Schultze and Avital [SA11]. These characteristics include that the interview is grounded in the participants' experience, the researcher need to acknowledge and value the participants' narrative, and the researcher is using a framework to guide the participant through the interview.

In order to follow the characteristics, interviews for this project will be in a semi-structured manner. A list of topics and questions are prepared before the interviews. Myers and Newman [MN07] suggest to script an opening, an introduction, key questions and a closing as a minimum before starting the interviews. The opening include an introduction of the researcher, and flow naturally into the introduction of the project and reason for the interview. In this project all the participants for interviews have already participated in the survey, and therefore know a lot about the project. The introduction will be short, but open for questions from the participant if it is unclear. In this section of the interview the researcher will introduce himself and ask permission to record the interview. If the participant give their permission, this can be revoked at any time and with no cause.

After the introduction of the interviewer and the project, the interviewer goes through the topic list. First in the topic list for this projects is questions to get to know the interviewees, such as "Can you talk about what you work with daily?". By starting with relatively easy questions, the interviewee start talking about simple everyday tasks as a warm up. The researcher continues to ask a little about the team, for instance questioning if any in the team has a focus on information security. By building the advance level of the questions little by little, the interviewer makes the interviewee ready for questions about the security and the risk in the project. The topic list continues to go through a few questions about security, one being "Who test the security of the project?". Eventually the researcher asks questions about risk management, for instance "Do you know what create risk in your project?". Before thanking the interviewee for his participation, the researcher asks if the methods chosen by the participant in their project have worked or not. The full interview list is found in Appendix B. The list is in Norwegian as this was the language the

interviews were conducted in.

Openness, flexibility and improvisation are attributes the interviews for this projects aim to achieve. One technique called mirroring allow the interview to follow the participants' narrative. In this technique the researcher uses the words and phrases from the participant, in order keep the participant describing their world in their own words. Listening, promoting, encouraging, and directing the conversation is then the role of the researcher. The interviewer is then prepared to explore interesting topics, and can look for interesting and surprising answers to help the project research.

The interviews will try to answer the research questions "What is the current state of practice for risk assessment in software projects?", "How does the practice of risk assessment affect software projects?", and "What are the benefits and drawbacks of doing risk assessment in software projects in practice?". Interviews were chosen as a method because of the advantage in retrieving in-depth answers. Ideally, interviews will provide an understanding and idea of how and why risk management is in use. , or why it is not.

3.2.2 Aspects That May Introduce Inaccuracies

According to Scultze and Avital [SA11] participants will usually share what they value and consider as a successful project. During the interview the researcher need to overcome some potential problems. These include the fear of embarrassment, and the fear of silence during the interview. Another problem that might occur is the possibility that participants are not completely open with the researcher.

Myers and Newman [MN07] summarise some problems and pitfalls with the qualitative interview in their paper.

- The interview is a social interaction and for some, if not all, of the participants it is an interaction with a stranger. Consequently, this can make the interviewee create an opinion under a time pressure.
- The researcher is not invisible. Because of this they may intrude and potential interfere with people's behaviour.
- The participant may find it hard to know how much to trust the researcher. An interviewee might then withhold important information.

Usually an interview is conducted in a time frame agreed upon before start. When the interview start the researcher might experience that the time frame is not large enough. Data gathering will then possibly be lacking, or the participant create an answer because of time pressure. Who the researcher choose to interview also come with potential problems. Where the researcher enters an organisation can have impact on who the participants become. If the point of entry is low in the organisation, the

researcher can have problems reaching senior managers later. Usually the researcher want a broad understanding of the organisation, and therefore need to be aware of elite bias. Elite bias concerns overweight of data from well-informed and high-status key informants in the organisation. As for the survey, the wording of the different questions is a potential pitfall. Because the questions might not be clear for the participants, and he thus do not understand what the researcher asks for.

Chapter 4
Results

Results for this paper was found by conducting a survey and eight different interviews with people who had answered the survey. The survey was sent out by e-mail as a self-administrative questionnaire, together with a consent form, and information about the project. It gathered information about the project type, the team, and the background of the participant. It also contained sections with security questions and questions about risk management. Answering the questionnaire took approximately ten minutes. At the end of the survey, the participants could choose if they wanted to participate in an interview for this projects. Section 4.1 show the results from the survey. The questionnaire can be found in its entirety in Appendix A, it is in Norwegian as this was the language it was distributed in.

Eight out of the 21 survey participants decided to participate in an interview. The interviews were used to get an in-depth understanding of the current state of risk management in Norwegian organisations today. As shown in Table 4.1 the interviews lasted between 13 to 38 minutes. All interviews were conducted by the researcher of this thesis, Heidi Svendsen. All interviews were recorded with the consent of the participants. In Section 4.2 the answers for the interviews are summarised and compared. Appendix C contains the full answers for every interview, and Appendix B contains the list of questions prepared before the interviews. Both Appendix B and Appendix C are provided in Norwegian as this was the language the interviews were held.

4.1 Survey

In this project the survey was in the form of a self-administrative questionnaire. To get a broad understanding of the marked, the population consisted of both companies who provides public services, develop their own product for sale, or provide consultants. Gathering the population consisted of sending out e-mails with information about the project, a consent form, and the self-administrative questionnaire. Recipient of this

e-mail where organisations from different fields who in some way develop software. Over 200 companies received this e-mail. Out of these 200, 21 organisations sent back the questionnaire providing the preliminary results. These acted as the basis for the interviews.

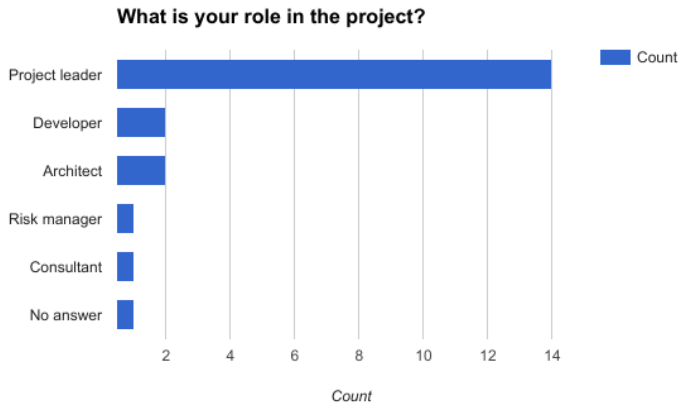

Figure 4.1: Answers to question 1 – "What is your role in the project?", from the survey.

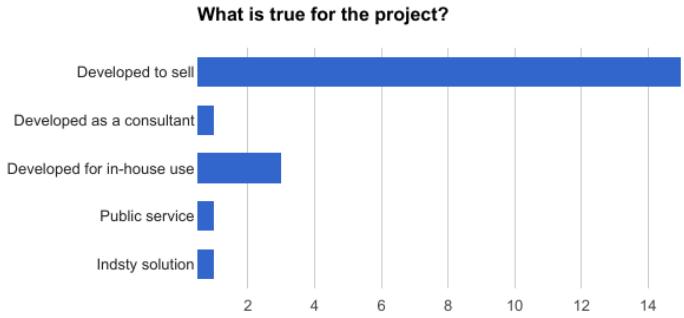

Figure 4.2: Answers to question 9 – "What is true for the project?".

In the information e-mail project leaders for development projects were invited to answer the questionnaire. Figure 4.1 show the answers to question 1, which were "What is your role in the project?". This figure show that 14 out of the 21 who answered had the role as project leaders, and the rest varied between developers,

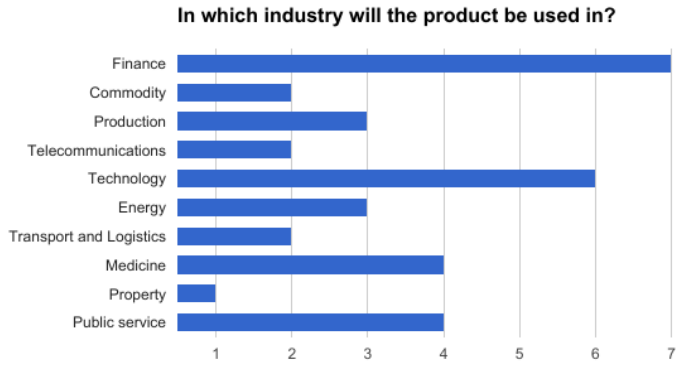

Figure 4.3: Answers to question 10 – "In which industry will the product be used in?".

architects, consultants, and risk managers. Question 9 asked if the project developed products for sale, if they were provided to the project as a consultant or if the project provided public services. As Figure 4.2 show, most answered that they developed products for sale. Sales are included in most industries today. To get an understanding of how the population for the questionnaire would turn out, question 10 asked in which industry the product would be used. Shown in Figure 4.3 the answers are distributed over most of the different fields, with a heavy answering load in finance and technology.

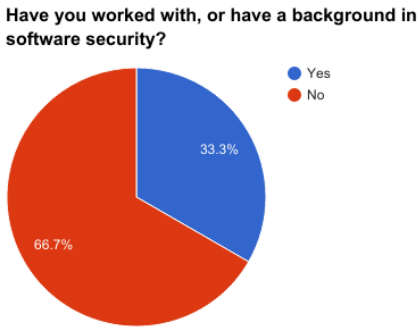

Figure 4.4: Answers to question 2 – "Have you worked with, or have a background in Software security?".

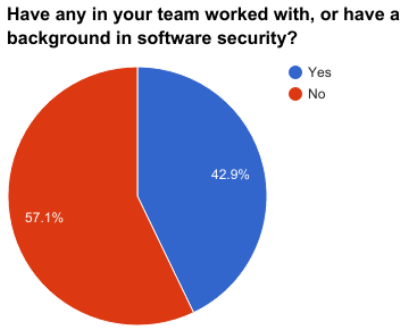

Figure 4.5: Answers to question 4 – "Have any in your team worked with, or have a background in software security?".

Size of the survey participant's teams varied from 3 to 150 people, most normal were teams of five to seven people. Question 2 and 4 asked if the participant of the questionnaire or any in his team had worked with security before. Answers to these questions are shown in Figure 4.4 and 4.5 respectively. The survey also asked if the teams got any training, either general security training, training by experts, voluntary role-specific certification, or mandatory role-specific certification. No one provided mandatory role-specific certification as an answer, and eight of the survey participants answered that their team did not get any security training. When it came to effectiveness of these methods, question 7 asked – "Which of these methods do you think are most effective?". Around half of the 21 participants answered that they think security training by experts is the most effective. Six answered that they think mandatory role-specific certification is the most effective. Which training methods performed, and the thought of the most effective methods are illustrated in Figure 4.6.

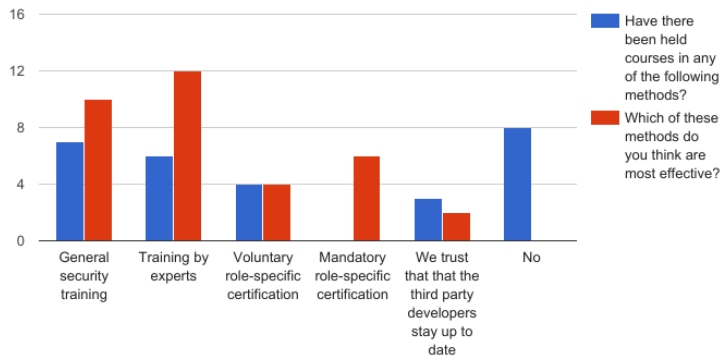

Figure 4.6: Answers to question 6 – "Have there been held courses in any of the following methods?" in blue, and answers to question 7 – "Which of these methods do you think are most effective?" in red.

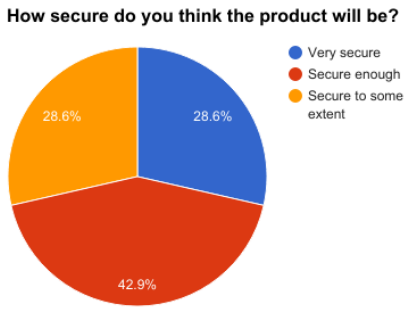

Figure 4.7: Answers to question 13 – "How secure do you think the product will be?".

At the start of the security section, the first question asked if the participant believed the product would need any form of security. All the participants answered yes. When they then were asked how secure their product would be, the answers varied between very secure, secure enough, and secure to some degree. This distribution is shown in Figure 4.7.

A system is only as secure as its weakest link [CW02], it is therefore important to do proper testing. Testing methods were out of the scope of the survey, but the

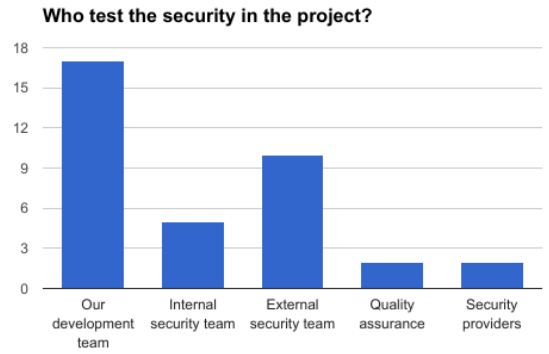

Figure 4.8: Answers to question 17 – "Who test the security in the project?".

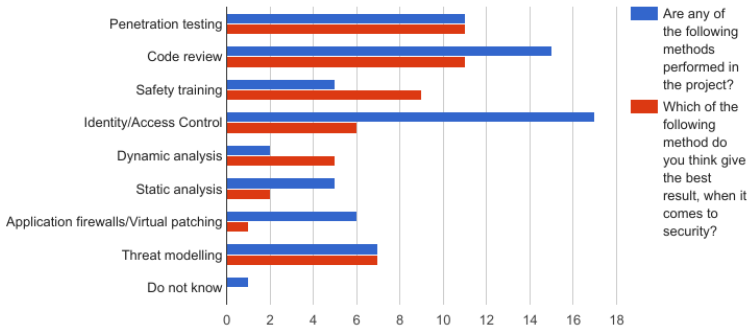

Figure 4.9: Answers to question 18 – "Are any of the following methods performed in the project?" in blue, and answers to question 19 – "Which of the following method do you think give the best result, when it comes to security?" in red.

participants were asked who performed the tests. Figure 4.8 show the answers to question 17 – "Who test the security in the project?". In this question multiple answers were allowed, and for many the team itself did the testing, but often an internal or external security team did some testing as well. At the end of the security section the participants were asked if some of the listed methods were performed in the project. The listed methods included; penetration testing, code review, safety training, identity/access control, dynamic analysis, static analysis, application firewalls/virtual patching, and threat modelling. After listing the methods performed, a question asked which the participant thought gave the best result. From Figure 4.9 it is shown that the biggest differences between these questions is for identity/access control and for safety training. 17 of the participants states that they

perform identity/access control, but only six think it gives the best result. Nine of the participants states that they think safety training gives the best result, but only five performs it.

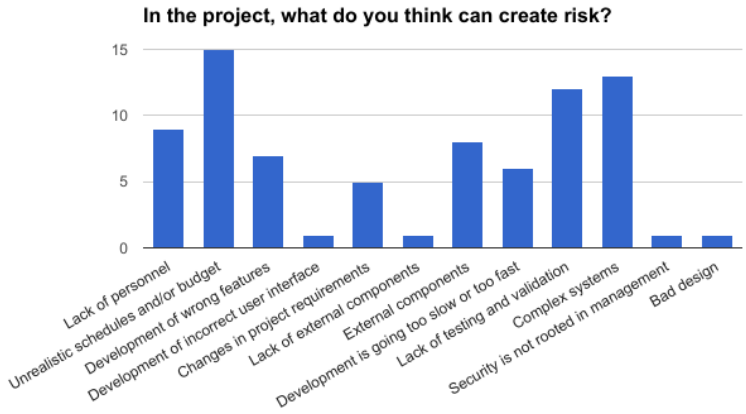

Figure 4.10: Answers to question 21 – "In the project, what do you think can create risk?".

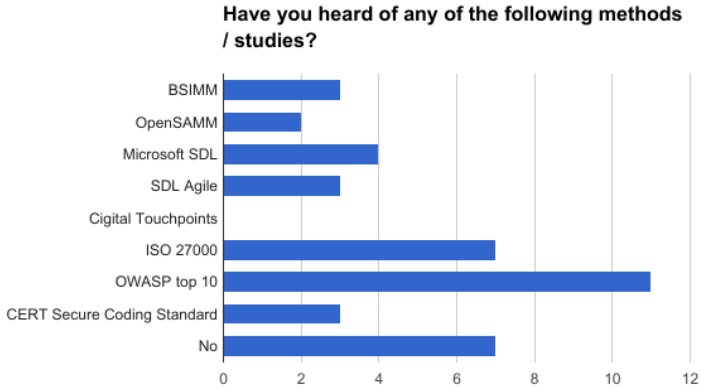

Figure 4.11: Answers to question 22 – "Have you heard of any of the following methods / studies?".

The risk section of the survey started with an open question on how risk was handled at the moment. 15 out of 21 participants decided to answer this question. Some stated that they started by identifying known risks. Others said that risks are reported along the way when they were found. While some said they did not have any

routines around risk handling. Before asking if risk assessments were performed, the participants were asked what they thought could create risk. Figure 4.10 show that the top three reasons for risk were thought to be; unrealistic schedules and/or budget, complex systems, and lack of testing and validation. Of methods/studies known to the participants OWASP top 10 was the most known. Seen on Figure 4.11 between two to four participants had heard of the methods/studies BSIMM, OpenSAMM, Microsoft SDL, and SDL-agile, all listed in Chapter 2. Out of the 21 participants in the survey, 62% performed risk assessment for their project, shown in Figure 4.12.

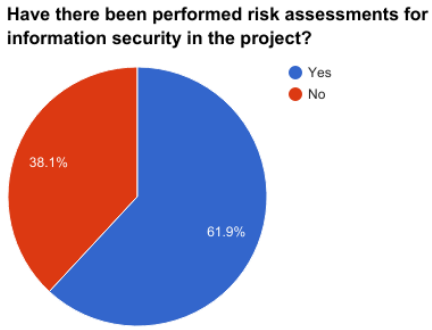

Figure 4.12: Answers to question 25 – "Have there been performed risk assessments for information security in the project?".

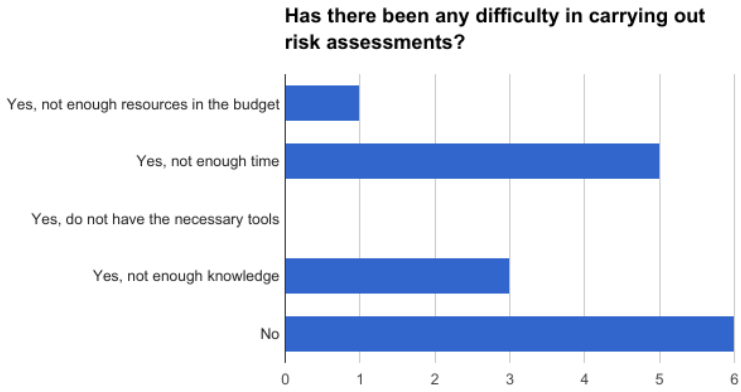

Figure 4.13: Answers to question 25.2 – "Has there been any difficulty in carrying out risk assessments?".

Most participants who performed risk assessments in the project did not have any difficulties. Figure 4.13 show that the ones who experienced problems said it was because they did not have enough time. In risk management it is recommended to perform a risk assessment more than once, because the risks will develop and change when the project progress. How often the projects reevaluated their risks is shown in Figure 4.14. One participant answered that he did not reevaluate the risk, but most of the other participants reevaluated when it fit with their schedule. For the ones who did not perform risk assessments, most gave lack of knowledge as the reason why. Figure 4.15 show the distribution between the three reasons; lack of time, lack of budget, and lack of knowledge. The question opened for multiple answers, so for some the reason was a combination of the three listed. No one gave the reason lack of tools.

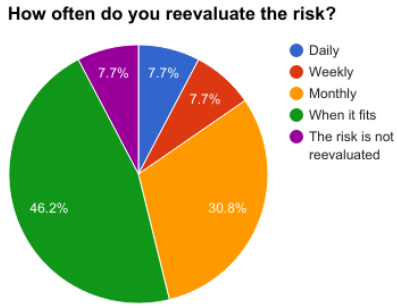

Figure 4.14: Answers to question 25.4 – "How often do you reevaluate the risk?".

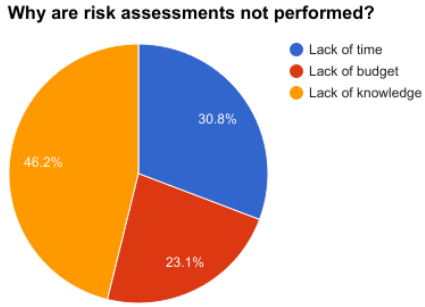

Figure 4.15: Answers to question 25.1 – "Why are risk assessments not performed?".

4.2 Interview

Last question in the survey asked if the participants were willing to be interviewed for this project. Eight interviews were conducted in total. Interviews were used to get more in-depth results than from the survey. It was a conversation with people working with software, both those who had used risk assessments and those who had not. The eight interviewees came from very different organisations, some from small companies in their start phase, others from big well known companies. Type of organisation also varied from projects who developed products for sale, projects who developed public services, and organisations who provided consultants. The variations in the population resulted in different comments, and in-depth studies of most of the survey.

	Skype or in-person	Interviewer	Role of interviewee	Interview time
Interview 1	Skype	Heidi Svendsen	Product owner	20 minutes
Interview 2	Skype	Heidi Svendsen	Project leader	18 minutes
Interview 3	Skype	Heidi Svendsen	Development leader	13 minutes
Interview 4	In-person	Heidi Svendsen	Consultant and software developer	20 minutes
Interview 5	Skype	Heidi Svendsen	Software developer	15 minutes
Interview 6	Skype	Heidi Svendsen	Team leader and software developer	18 minutes
Interview 7	In-person	Heidi Svendsen	Technical project leader	18 minutes
Interview 8	In-person	Heidi Svendsen	Position in the security group	38 minutes

Table 4.1: Details of the interviews conducted.

Five of the interviews were conducted over the platform Skype. Next to the difficulties of holding an interviews, the technical aspect of Skype had some difficulties as well. The video chat sometimes froze, making either the interviewer or the interviewee repeat himself. Other times the sound quality were not the best, making the quality of the recorded tape worse. A sixth interview was scheduled for Skype, but because of technical difficulties it had to be rescheduled to an in-person interview instead. Difficulties with the interview are explained in Section 3.2.2 in Chapter 3. Including the rescheduled interview, there were held three in-person interviews. All the interviews were recorded with a tape recorder, with the consent of the interviewees. Details of the interviews are provided in Table 4.1.

Interviews were conducted in a semi structured way. Meaning some of the questions were prepared beforehand. They all started the same; after a presentation about the project and the interviewer, the interviewees talked about their project and their background. They continued to talk about the teams, before the interviewee and the interviewer had a longer conversation about the security in the software and risk management. For the last part of the conversation the interviewees talked about what they found relevant, and the interviewer only guided the conversation to some degree. The interviewer made sure to go through the prepared questions, but other than that kept the conversation around the answers from the interviewees. This resulted in different answers, because the interviewees focused on different things under the interview. Even though there was differences in the answers some similarities can be found and all of the interviews had interesting viewing points on the different topics.

The organisations of the different interviewees varied a lot in the size, but still the team sizes remained at the same level for all of them. Three of the interviewees told that they usually had consultant as well as their own employees for the team. All agreed that a team of four to seven were the ideal team size. One said they used to keep the number of team employees under 7 because they ran agile teams. When asked if any in the team worked with security, the answers varied. One interviewee said that none of them worked with security, but in the start of the project they hired security consultants for a short period. Interview 8 had 4 interviewees, were three of them held a position in the organisation's security group. They explained that they had two different roles as security advisers in the projects; they worked with both the security architecture and risk analysis. In one of the organisations some of the developers had a role they called security champions. This meant that they have an extra focus on security and usually had an education in security development. Interviewee 2 pointed to the organisations security head as he were responsible for the security, both internally and externally. In this organisation he helped the technical employers responsible in the different projects. Interviewee 1 said they did not have anyone working directly with security as it was not their responsibility. For them it was the customer who were responsible for the security as the product were installed in their environment. The customer had to take care of who had access to which data and to secure their environment.

When it comes to security training through courses and seminars, the organisations interviewed did little of that. Training mostly consisted in being taught in the platforms used and sold. Interviewee 4 said that their consultants could attend which conferences they wanted and sometimes security was a theme at those, but they did not have any mandatory security training. The organisation in interview 8 had a course on vulnerabilities on the web and for services over HTTP. The interviewees in this interview explained that it was their responsibility to inform the employees about the importance of good security work. They had implemented the national

security month of October[1] and started with a training method called NanoLearning. NanoLearning [Jun] give the employees of the company small courses they can do on a computer during the year. This was given to all the employees, not just the developers. Also the organisation for interview 6 gave all their employees mandatory NanoLearning. Special for the developers was that they have internal courses as well, and small lectures about specific themes in security.

Aspects concerning security in the development were different for the organisations. Interviewee 2 mentioned the legal aspects of security and privacy, they made sure that their employees were kept up to date on the on these aspects. For their payment solution they had a third party implement it, avoiding some of the certifications needed for that type of solution. Similarly, interviewee 5 said they had a third party protect the user information. In order for this solution to work they had a contract with the third party and trusted them when it came to how secure it was. Further he said that the user information they collect were not of a sensitive matter, only the user's name and e-mail address. Interviewee 7 said they mostly focused on the communication between the application and the backend, which used a secure protocol and was encrypted.

It exist many different methods to ensure that a product is secure. During the interviews this was one of the themes which surfaced. Interviewee 3 explained that the organisation had try to make a process inspired by the Microsoft SDL, but it was still in the earlier stages. Also the organisation in interview 6 were inspired by the Microsoft SDL. They had both a secure-SDLC and a SDLC. The secure-SDLC told which activities to perform and when to perform security requirements and risk assessments. It was not integrated in the SDLC, but the secure-SDLC pointed to phases in the SDLC. The interviewees in interview 8 provided their developers with standard components which solved a lot of the functionality like authentication, authorisation, and access control. Their developers leaned on the security department when it came to methods and templates. In interview 1, the interviewee already explained that they did not do much when it came to security as it was the customer's responsibility. During the conversation he said that they did track changes in their program, e.g. who did what. So there was always a way to track if someone did something they were not supposed to, either on purpose or by accident. Their customers were both Norwegian and non-Norwegian companies, the interviewee had experienced the difference between both domestic and international customers. Norwegian organisations were more trusting and open of their employees, one employee do a lot of different tasks and therefore need a lot more access than the employees of a international company.

Common for all organisations interviewed, except for interview 5, were that they

[1]Information about the national security month in Norway can be found on [Nor].

conducted testing internally. Some of the organisations also hired external help to test the product before putting them in production. But when asked if they knew which treats they were exposed to, again the answers varied. Interviewee 3 felt this area were conducted beside the developers, and not together with them. The organisation for interview 8 held an updated list over different threats, while interviewee 4 told they had consultants helping them find threats and to evaluate the risk. For an organisation with a lot of different software products and some hardware products, the different threats varies a lot, both in severity and size. This was the case for the organisation in interview 6, they had threats in the whole spectrum and it all depended on the service talked about. Still, all of the projects interviewee 6 had held a list of threats relevant for them. The other organisations interviewed did not know how, or did not have a process, to find the relevant threats.

Interviewee 4 did not use risk analysis, but still had some ideas on what could create risk in the project. Three things he mentioned were; the developer create risk with his code, the environment where the application run create risk, and risk is created by the down time of the system. He said he would not start to use risk analysis himself. If he needed it there are experts to be hired. On the other hand interviewee 2 said that the biggest source for risk is the human interaction with the system, and one can not plan for mistakes humans make. For him the decision of doing a risk analysis depend on the customer. Some customers were very easy to work with, he said. When they held weekly meetings and they knew what to go through, it was easy to maintain the risk document. He also had customers who were more unpredictable and very dynamical, and maintaining a risk document for these type of customers become somewhat impossible. Interviewee 7 did not do any risk analysis in the development, but said they would have to change this because of the new Eureopean Union (EU) law which make documentation on risk evaluation much stricter. During the fall they would implement frameworks for new risk evaluations and assessments. One of the organisations not using risk analysis said it was because it was not their application. Their customers choose to use their product in the way that they do, therefore it was up to them if they wanted to do a risk assessment or not.

At the end of the interviews the interviewees were asked if they could think of positive or negative sides by doing a risk analysis. Most saw it as useful, but it demanded to many resources. Usually a risk analysis only provides a result, being for instance small problems the developers need to fix, better awareness of the security threats, or plans for problems that might occur. For some interviewees the risk process produced documentation useful when they needed to defend the architectural and development decisions they made during the project.

Almost all agreed that they would like to use some kind of risk analysis, but it was

not prioritised high enough. For the product owners, security become a pain if they wanted to keep their deadlines, and it was more important to get the products to work and out for sale. Interviewee 2 said the focus should not be on whether or not to use risk modelling tools, but to figure out how to solve problems that arrived with the risk. As Boehm [Boe91] said in his article, one of the interviewees in interview 8 reasoned the same when it came to risk analysis; *" ... the value of it is the same as for development, the earlier you find the mistake the cheaper it is to fix"* [2].

[2]Not a direct quote as it is translated from Norwegian. The quote can be found in Appendix C.8, last bullet point under question 17.

Chapter 5
Discussion

In 2010 David Geer wrote an article called *"Are Companies Actually Using Secure Development Life Cycles?"* [Gee10]. As part of his paper he used a survey from the consultancy firm Errata Security, their survey received 46 responses. One of the questions in Erratas survey were similar to question 22 from the survey conducted in this project, "Have you heard of any of the following methods / studies?". Errata asked if the respondents were aware of any of the following SDLs; SAMM, BSIMM, Microsoft SDL, Microsoft SDL-Agile, Securosis SSDL, or CLASP. Answers they received are shown in Figure 5.1 [Gee10], and to compare, the answers from question 22 in this project's survey are shown in Figure 5.2.

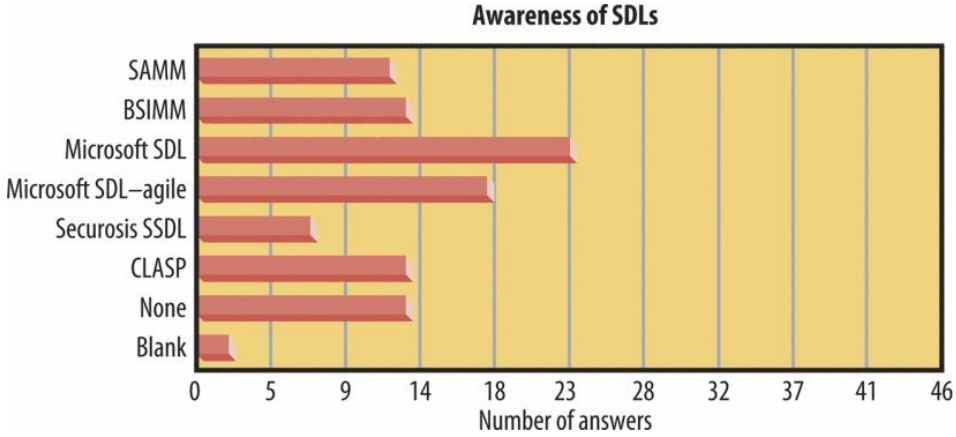

Figure 5.1: Answers, out of 46 respondents, to the awareness of different SDLs, from a survey conducted by the consultancy Errata Security.

To be able to closer examine the differences, Figure 5.3 show the results as percentages of the respective respondents. Seen from this figure, over 50 % of the respondents in Geer's article [Gee10] were aware of Microsoft SDL, and only 19 % of the respondents from the survey in this project. The trend is visible for the other lifecycles as well, a

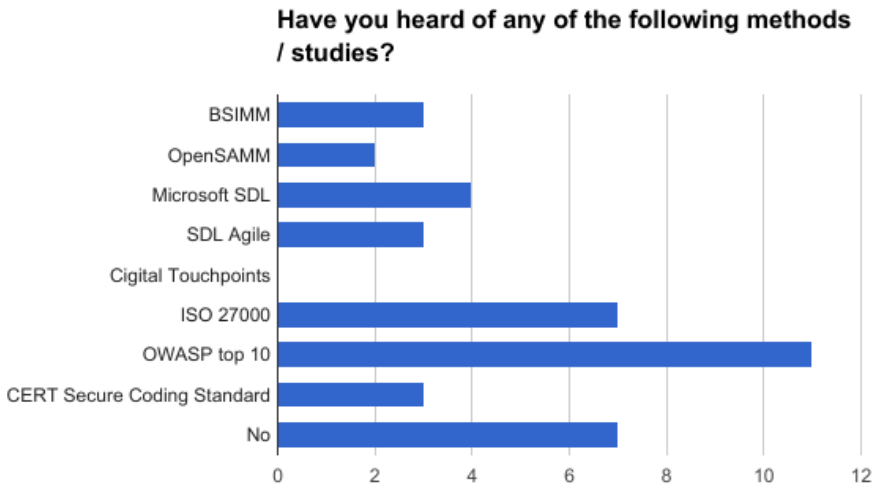

Figure 5.2: Answers, out of 21 respondents, to question 22 in the survey conducted in this project.

larger percentage of the respondents in the Errata survey were aware of the different lifecycles. In the survey conducted for this project the percentage was under 20 % for all of the lifecycles. Figure 5.2 show that the respondents from this survey were more aware of OWASP top 10 and ISO 2000. One of the reasons for this might be the crowds the surveys were shared in. Erratas survey were shared on their security blog and on two security conferences, while the survey for this project were sent to development departments in different companies. Developers reading security blogs and attending security conferences might be more interested in security than the average developer. Because of this it is natural that they are more aware of the different security methods for development.

Out of the 21 respondents in the survey for this project 8 respondents did not perform risk assessments for their projects, as shown in Figure 5.4. Four of them had only heard of OWASP top 10, three had not heard of any of the listed methods/studies, and only one had heard of Microsoft SDL. Drawing a conclusion from this show that knowledge of SDLs most likely result in knowledge of risk management. This may bring a discussion about the research questions raised in the beginning of this paper. A discussion from the data given in this paper, can give an idea of the current state of risk assessment in software project. The data gives an idea how risk assessments affect these projects, and how managers think around both negative and positive sides of risk assessments.

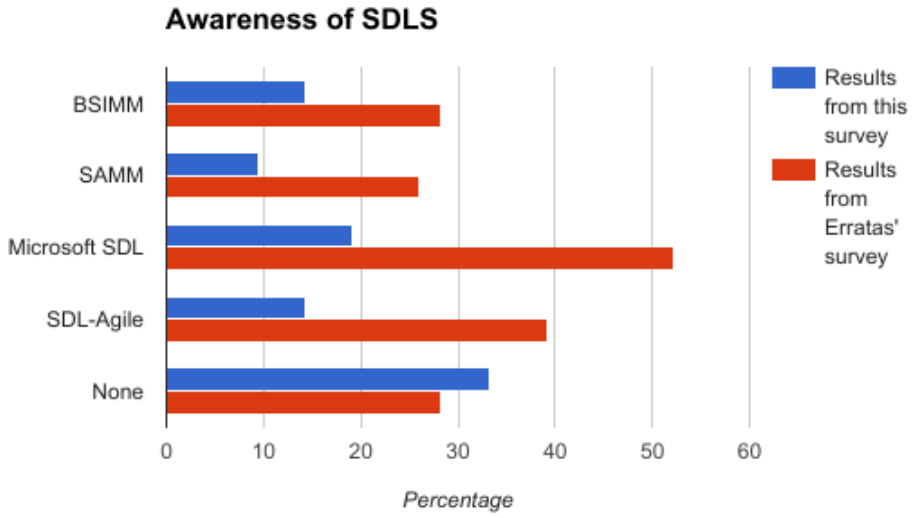

Figure 5.3: Comparison of the answers from Erratas survey and the survey in this projects. Results are here given as percentage of the respective respondents.

5.1 Current State of Risk Assessment in Software

From the survey, 38 % of the respondent answered that they did not perform any risk assessment for their projects. Presentation of the percentage of the respondents who performed a risk assessment for their projects are shown in Figure 5.4. In numbers, eight respondents said they did not perform a risk assessment. Still three of them answered the previous question 20 – "How is the risk in the project monitored and handled at this time?". One respondent said that the risk was identified early in the project and the solutions for them where it was possible. This was their only risk assessment, as they did not perform a continuous analysis. The other two answered the question for general risk instead for software security risk. They did risk analysis for the marked, technology, and the development processes, usually this analysis were handled by the project leader. Still, the one who answered that his organisation did not perform risk analyses because it was not a continuous analysis, performed one kind of risk analysis. Initially, a risk analysis should continuously be updated to be able to handle rising risks. But, it is still a risk analysis even if it is only performed once in the project, it will just not be updated for any new arising risks. Conclusively, seven out of the 21 respondents are not performing risk analyses.

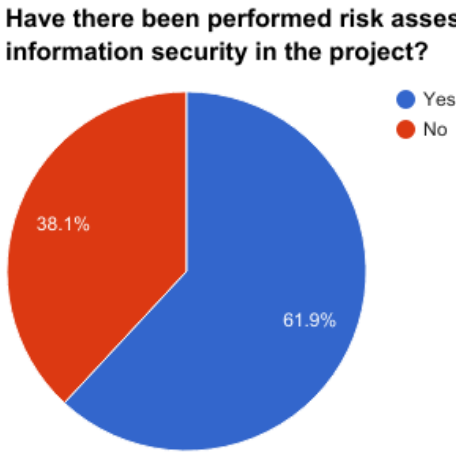

Figure 5.4: Percentage of the respondents in the survey for this project, who performed risk assessments in their project.

Between the other 13 respondents who performed risk assessments in their projects, 10 of them answered question 20. Only one respondent specified that they initially started with a workshop to find risk, after this workshop they continuously handled existing and new risks during the project. Mostly the other answers explained that they did risk analyses continuously during their project. One way of doing this was to strategically reevaluate the risk upon reached milestones, another way is to let the developers find and report the risks during the coding and then together find a mitigation strategy. Others follow for instance the Payment Card Industry Data Security Standard (PCI-DSS).

Others said they did perform risk assessments, just not them self. One said it was done by a third party who was operating the system. Another organisation did risk assessments for information security in the product when it was relevant for them. Operational risk analyses of security such as infrastructure and firewalls, were conducted by other groups within this organisation. As for the last survey respondent, he focused mostly on personal data. Their risk analyses were directed towards how an attacker could retrieve personal data from users in their system. This is a good approach when the assets of the company is personal data, but as for this respondent it seemed from his answer that they had a few other assets as well. Then they should also perform a risk assessment for these assets.

From the results of the survey it seems that most organisations perform one kind of risk analysis, at least when the organisation has passed their starting phase. But with further investigation, in the form of interviews, it seems risk analysis in the survey could be misdefined as project risks. Few of the organisations who answered that they did risk assessments in their software projects were in fact performing risk assessments for the project itself, and not software security risk. This means the organisations still have features to implement in their risk assessments. Knowledge of project risk methods will help in implementing risk assessment methods for software security, as the idea of it often is the same. For organisations with a lifecycle methodology, implementing risk assessments should not be to hard in practice. Still for the first projects it might be a different way in thinking, and it might demand more resources than it saves later. As with everything else a risk assessment will not be performed perfectly at the first try, it requires practice. With practice it can be seen that doing a risk assessment can help patch the security risks before an attack happens.

5.2 Risk Assessments Affect on Software Projects

Most of the interviewees agree that a risk assessment gives the organisation the opportunity to be prepared for unintended events that may occur. But an organisation is not just ready for an expected unintended event, but also more prepared to handle unexpected events. An organisation that have a plan for expected events have the training to make this plan, and will therefore be more prepared for the unexpected as well. If the organisation sell their products to a customer, the customers are also affected by an risk assessment. When the customer see that the organisation is prepared for events that may occur, it might be easier to sell the product.

Interviewee 2 explained that the risk assessment had an effect on the culture in the organisation. Every employee helped each other with knowledge and skills. They shared the knowledge of what they learned from the different phases in a project and would try to help each other in challenges, even if they were security related, risk related, or development related. By doing risk assessment they learned that for them the biggest risk were the human aspect of projects. In order to try to lessen this risk, the employees leaned on each other and learned together. For them it was important to be united in the issues. Even though interviewee 2 is the only one who discussed the importance of human mistakes, it is not less important. As interviewee 4 said, the one who writes code create a risk just by this code. It is hard if not impossible to prepare for all the different human mistakes which may arise. But it is still possible to prevent a number of human mistakes, and the risk assessment help the organisation see which human mistakes they can prevent.

Performing risk analyses may also have an effect on the developer. Interviewee 6 said that when he got different security courses, he experienced getting a different

mindset as a developer. Before he could add lines of code writing output to the log, not thinking this could be used in any malicious attacks. After the courses he had, he became more thoughtful of the output his code produced. He said, since the risk evaluation and the risk assessment might change developers mindset, it is important to include them in the process of finding and assessing risk. They may not come up with new and important risks, but they might remember them when writing code, and therefore avoiding some risks. Interviewee 7 did not feel he had changed his mindset after conducting strict risk assessments in one of his previous projects. He said he knew about the different methods of risk management now, in case he needed to do a risk assessment. Still he did not believe he would need to use this knowledge in the near future. The organisation in interview 7 did not prioritise security at this moment, as they focused more on getting their projects to work. Still interviewee 7 acknowledged that this certainly would be harmful in the long run. In order for the risk assessment process to change the mindset of the developer, it need to be performed continuously to keep it on their minds. It may be easier for a developer who changed position to a security developer to change his mindset after a few courses, than for the average developer. Still in the projects using risk assessments in the beginning of the projects, the developer is more observant when it comes to risks. This might help prevent human mistakes, and as the risks change, they should update the risk assessment in order to keep the developers up to date on the risks as well. For projects where no risk assessments are performed, or the developers are not included, it may be harder for the developer to be alert when it comes to the different risks which follow from the code.

Effects on the software project might not only be positive. A risk assessment might be done in great detail, and the ones who perform it may have a great deal of experience. On the other hand it might be a short risk assessment, which is both lacking and not thorough enough. The ones performing the risk assessment might not be experienced enough, or the courses needed might be lacking. In these latter cases, the risk assessment would most likely suffer of lacking information. In an organisation where the risk assessments are in use in the projects this may have an effect on the security. Either that the project is not ready for an event, do not expect an event to occur, or may not know what risks they are facing. This has the most impact on projects who do not fully reevaluate the risk. Projects who reevaluate the risk may make changes and new measures. A lacking risk assessment is also a risk by it self.

Interviewees who did not perform risk assessments still had opinions about it. One said that he felt the risk assessment was conducted next to the development and not together with it. This might not be the optimal solution as a risk assessment should include risk of the software as well. For some organisations it seemed that this might be the case, mostly because of lacking resources and knowledge. Developers should

be more included in the assessment, but they do not suggest any solution for how this might be realised. There was also one interviewee who said that they had consultants in the beginning of the project assessing the project and suggestion different things to be done. For them risk assessments have by now not been a prioritisation, because they felt it would take to long time, and needed the time to finish their product. One can argue that the lack of spending time on a risk assessment might result in more loss of time if something goes wrong. If one have a risk assessment, a few scenarios have been provided a plan in order to quickly fix what happened and continue with the project. The organisation who used consultants also explained that all their data were saved in a cloud provided by a third party. When asked if they had any plans of what to do if this data became lost, they simply answered no and continued to explain that if that happened the project would be dead.

5.3 Benefits and Drawbacks

During the interviews one of the questions were if the interviewee could think about benefits and drawbacks of doing a risk assessment. As for the drawbacks most said the biggest were the fact that a risk assessment requires resources. As security got under 5 % of the budget in most of the projects, see Figure 5.5, there was not that much in the security budget for a risk assessment. The interviewees who did not perform a risk assessment, said it was because they did not want to prioritise it over other security aspects. One said that they would like to do a risk assessment, but none prioritised it high enough to spend a lot of time on it. For them most of the budget went to getting their product to work and out for sale, and at the same time keep the different aspects within the laws. He claimed that they would spend time and resources on risk assessments when the product were out for sale and working. This was a small company and in the starting phase. From the other interviews held the organisations who performed risk assessments were relative big and well established organisations. From this it would seem that it takes a few years before risk assessments are a priority.

Drawbacks also concerns the budget surface when one performs a risk assessment. A risk assessment will give output in the form of a list with aspects in need of action. Usually these actions are prioritised in how urgent they are, and how severe a loss from this shortcoming will become. Companies with a small budget for security might want to give these resources to aspects they know they need and not to whatever is on top of the prioritised list. It might be a fear that the security needed comes to far down on the prioritised list, and then the resources have run out before they arrive at that point in the list. This show that a risk assessment might be quite resource intensive. Because of this one of the interviewees in interview 8 said that they did not have the capacity to do a risk assessment in all of their project, they needed to

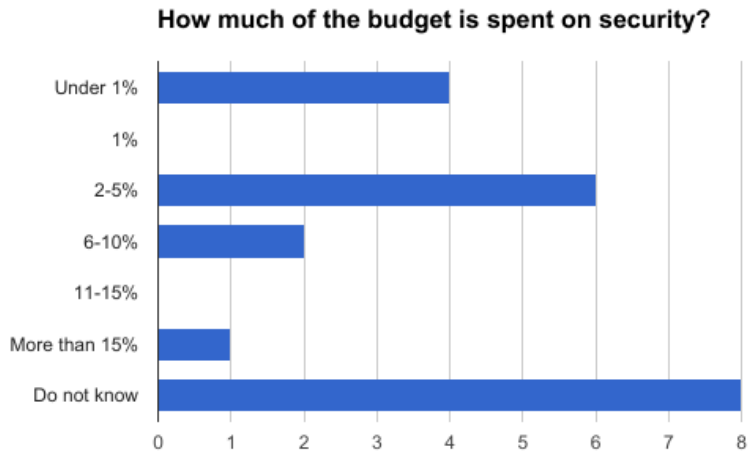

Figure 5.5: Answers to question 14 – "How much of the budget is spent on security?".

prioritise which project to perform a risk assessment in. For them the resources were the biggest obstacle.

Except from the drawbacks concerning the budget, interviewee 2 included the drawbacks of the amount of work a risk analysis takes. Keeping a risk assessment requires continued work and updating. It will require standardisation and maintenance. If one forget to keep maintenance of the document, the standardised methods are then outdated, a lot will change over a short period of time in development. Before doing a risk assessment one must do the groundwork, and have a plan of what to do during the project. One aspect to think about is who will take time out of their work to maintain the risk assessment. Developers already have the development job to do, the managers have a lot to do, and will not prioritise maintenance of the risk assessment document. Then one is back to the budget drawback; is there enough budget to hire a risk manager to update the risk analysis and standardise solutions to events that might happen?

From the interviews it seems that the interviewees thought more of the benefits of doing a risk assessment. One said that next to the economical drawbacks, he could not see any more drawbacks as the risk assessment only produce a result. One benefit was that the risk assessment helped the organisation be clear and open to the customer. The risk assessment standardise a lot of solutions to events that might

arise. Because of this the risk assessment help to be prepared. Both a plan A, and a plan B can be planned for an event. It also gives an idea of expected events, meaning that the organisation and the developer might avoid the event all together.

Some project might attract the eye of the public. By using a risk analysis one have to document the different risks the project decide to take, and how other risks are avoided. By having all decisions documented it is easier to show to the public why different decisions were made, and how problems were avoided. Projects which attract the eye of the public are most likely a project which is dependent on the trust of the user. The benefits of doing the risk assessment will therefore weigh up for the economical drawback.

On the other hand, not doing the risk analysis has its benefits as well. When the risk assessment have not been performed the project learns to be flexible, and to quickly react to changes and events. The developers in the team get comfortable to make mistakes, and quickly fix them, either by himself or with help from others in the team. If an event occur in this project they do not have to look up the event in the documentation to know which action is required. This makes the whole project dynamic and fluid. The drawback of being dynamic is that the project will not perform a control of the different risks. A project leader is expected to perform different controls during the project. By not having the documentation, decisions might be questioned not to live up to the expected result. While there are benefits and drawbacks to all decisions, including the decision to do a risk analysis or not, the decision most likely depends on the organisations internal rules and the project leaders experience and personality. Most importantly is how the organisations handle different problems that occur.

5.4 Risk Assessment or not Risk Assessment

Using methods such as a survey and interviews may give subjective answers. One can ask direct questions about what a company does and how different stages of development is performed, and get a clear picture of the processes in said organisation. Still the researcher is dependent on the honesty of the research participants. When asking for an opinion, or how well a stage in the development is performing, the answers received is often the subjective meaning of the research participants. During this research project a subjective problem occurred when trying to figure out if using risk management would improve the security. When asking the participant who used risk assessments in their projects they assured that it helped when it came to security. And, when asking the participants who were not using risk assessments in their projects they assured that their security would not become better with a risk assessment.

Results from the survey ended up focusing mostly about what organisations performing risk assessments are doing. Because of this the results between software projects using risk assessment and software projects not using risk assessment, does not give a conclusive result. Together with the subjective answers from the interviews, this result in an impossible task to find differences between these two types of projects.

One possible solution to this would be to refocus the survey to questions that would show the differences, and not focus so much of finding the current state of risk analyses. Another, and possibly better solution to this would be to perform testing on the participating organisations. As this was not done for this project a possible way to perform such testing is discussed in Chapter 7.

5.5 Difficult Aspects During the Research

Information for the project, the consent form and the survey went out to over 200 different companies. Out of them around 10 % gave a positive response and decided to participate in the survey. Hill [Hil98] wrote that a sample should be 10 % of the population in order to do descriptive research, but for a small population 20 % may be required. From this, up to 40 participants were desirable for the survey. But Hill continue to list three reasons were a small sample size are justifiable. One of the reasons listed was cases were in-depth studies are a part of the research. This includes research which requires interviews as a methodology.

A small sample size is therefore justified by the interviews held during the research. Desirably, all the survey participants should partake in an interview. As it was voluntary to do an interview, eight of 21 signed up. Still the survey and the interviews together gives an understanding of the current state of risk analysis in software development. As the interview subjects mostly were people who had worked a few years, they all came up with a few thoughts about risk analysis. These thoughts concerned both why risk assessments are not used broadly, especially in smaller companies, and what risk analysis could give back to a project. A researcher will at most times want more research participants, as it is for this project as well. Still these justifications show that with the participants who partook in this research can give a descriptive view into how risk analysis are performed in organisations today.

One of the interviewees pointed out that the survey could be misunderstood. The part focusing on risk could be understood as general project risk management, and not risk management for software development. This might not have been thoroughly explained in the survey itself, but were explained in the information e-mail which were sent out. Still he went back and changed the answers when he realised the part was about risk management for software development. None of the survey results from this part was notably different from any other, and therefore the comment did

not cause any action to be taken. The comment was taken to heart, and if there were to be a new survey, it would specify more clearly in the survey itself that the part concerning risk management is actually about risk management for software development.

Mentioned in Section 3.2.2, during an interview the researcher is not invisible. During the interviews held in this project the researcher found the interviewees to be open and honest in their answers. Some were hesitant to answer specifically why they did not perform either testing or risk assessments. But the belief is more that they did not know rather than that they did not want to answer. One of the pitfalls encountered were that the researcher felt it difficult to stay entirely objective. Sometimes the interview turned more into a conversation than just a question/answer interview. Other times the interviewee did not understand the question being asked, and the researcher needed to explain the question in more detail. When this happened, it was easy to fall into the trap of over explaining. During the write up later in the process, these parts of the interviews were examined closely to see if it were consistent with the rest of the interview. As it were most of the time, this pitfall was then not considered any further. The researcher is in the opinion that a conversation during the questioning were helpful, as it engaged the interviewee to share information previously not thought about as an answer to the asked question.

Chapter 6
Conclusion

From the results of the survey it seems that most organisations perform one kind of risk analysis. A few of the organisations who answered that they did risk assessments in their software projects were in fact performing risk assessments for the project itself, and not software security risk. But overall, a majority of the organisations questioned for this research perform a software security risk analysis. It is possible to draw a line between organisations performing risk analyses and the size of the organisation. Organisations performing risk analyses were the largest organisations, and the ones who had software security risk assessments implemented in their over all process. These are the companies who made risk management mandatory for their projects.

A risk analysis may have many different effects on a software project. One of them might be the on the culture in the organisation. In one of the researched organisations, performing a risk assessment opened up for a intellectual sharing culture. The risk assessment let the employee show what they were good at and get input from others. Every employee help each other with knowledge and skills. They shared the knowledge of what they learn from the different phases in a project and try to help each other in challenges, even if they are security related, risk related, or development related. Another effect risk analyses may have is the effect on the mindset of the developers. Because of this an interviewee pointed out that it is important to include the developers in the risk assessment process. Not because they might come up with the newest or most important risks, but because it might help prevent human mistakes.

Most of the interviewees agreed that the biggest drawback of doing a risk analysis was the economical. A risk assessment takes time to perform and finish, and it should be updated during the project. This takes time and becomes an economical aspect of the project. For projects lacking risk assessment experience or security experience, experts are usually hired. Projects with a limited budget may not prioritise a risk analysis if the benefits of doing one is not clearly laid out.

As for benefits of a risk analysis, the interviewees came up with far more benefits than drawbacks. The benefit that most of them seemed to be focused on was the fact that a risk analysis let an organisation be prepared for an unsuspected and unintended events. By having a risk assessment plan, a few scenarios have been provided a plan in order to quickly fix what happened and continue with the project. Being prepared for an unintended event also prepare the team for an unsuspected event. Because the team already know how to set up a plan for events that might happen and can therefore quickly get in the mindset to efficiently fix the occurred unsuspected event.

Still it might seem that risk assessment itself is not the most important aspect in being ready for an unsuspected event. There exists a number of methods to prepare for unintended and unexpected events, where risk management is one of them. For an organisation it might seem that it is not how risks are found or what degree of impact the risk will have. The important aspect of risk management is how the organisation define risk, and how they choose to solve the risk related problems before and when they occur.

Chapter 7
Future Work

In continuation of this project I want to answer the fourth research question – "What are the differences between software projects using risk assessment and software projects not using risk assessment?". During the time this project ran I realised that methods such as a survey and interviews would not answer this question. Research participants have a subjective opinion when answering this question, and the questions were not designed in a way that showed differences in a satisfying way.

To answer the fourth research question I would use the method of risk based penetration testing. This method involves defining business goals, priorities and circumstances. Then the tester identify both technical and business risks and link the risks up to the different business goals. The tester does this in order to know where the attacker will gain the most from a successful attack. After the risks are identified, they are ranked and prioritised. For the RMF the next step would be to mitigate the risks found in order of prioritising, but the tester want to figure out if the identified risks are indeed risks for the product and organisation. The list of prioritised risks are used as the testing list, where the risk with the highest prioritisation will be tested first. The tester keep a detailed document of the aspects of the products tested, and if the tests were successful or not to give back to the organisation.

Because the question asks for differences between projects using risk assessment and projects not using risk assessment, the organisation tested should be as similar as possible. The difference being the use of risk assessments. Using the survey and the interviews I will find two and two similar projects and test against each other. As this task requires a lot of time to realise, it went out of the scope of the 20 week period given for this master's thesis.

One of the interviewees mentioned that their organisation would focus more on risk analysis in 2018 when the new EU reform take effect. The regulation of the reform will apply from 25 of May 2018. This regulation is a step to strengthen the fundamental rights of citizens in the digital age [Comb]. The regulation will apply to

organisations and people based in the EU and organisations based outside, if they collect or process personal data of EU residents. Personal data is in this capacity defined as *"any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address."* [Coma]. The reform have clear rules for businesses where one of these rules is the urge for a risk-based approach. The rule will avoid a one-size-fits-all method, but urge the organisations to tailor a risk-based approach to the respective risks when it comes to personal data protection.

In continuation of this project I also want to catch up with the interviewed organisations after the new EU reform take effect. It would be interesting to see if any of the projects started doing risk analyses because of it. An aspect to look into would be the thoughts after a change and if they find the risk analysis useful. Another aspect would be to check back on the benefits and drawbacks to see it the interviewees have changed their views there.

References

[And10] Ross J Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2010.

[Boe91] Barry W. Boehm. Software risk management: principles and practices. *IEEE software*, 8(1):32–41, 1991.

[CD05] John Chirillo and Edgar Danielyan. *Sun certified security administrator for Solaris 9 & 10 study guide*. McGraw-Hill, Inc., 2005.

[Cha09] Pravir Chandra. Software Assurance Maturity Model. Technical report, OWASP, 2009.

[Coma] European Commission. Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. Available at http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, Last accessed: 2017-05-22.

[Comb] European Commission. Reform of EU data protection rules. Available at http://ec.europa.eu/justice/data-protection/reform/index_en.htm, Last accessed: 2017-05-22.

[CW02] Hao Chen and David Wagner. MOPS: an infrastructure for examining security properties of software. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 235–244. ACM, 2002.

[DWSB+09] Bart De Win, Riccardo Scandariato, Koen Buyens, Johan Grégoire, and Wouter Joosen. On the secure software development process: CLASP, SDL and Touchpoints compared. *Information and software technology*, 51(7):1152–1171, 2009.

[FJ13] Floyd J Fowler Jr. *Survey research methods*. Sage publications, 2013.

[Gee10] David Geer. Are companies actually using secure development life cycles? *Computer*, 43(6):12–16, 2010.

[Hil98] Robin Hill. What sample size is "enough" in internet survey research. *Interpersonal Computing and Technology: An electronic journal for the 21st century*, 6(3-4):1–12, 1998.

[IRG08] IRGC. Introduction to the IRGC risk governance framework. Technical report, International Risk Governance Council, 2008.

[Jaa12] Martin G. Jaatun. Hunting for Aardvarks: Can Software Security Be Measured? In *International Conference on Availability, Reliability, and Security*, pages 85–92. Springer, 2012.

[Jun] Junglemap. NanoLearning: Learning made easy. Available at http://www.junglemap.com/, Last accessed: 2017-05-03.

[KKS12] Mumtaz A. Khan, Shadab Khan, and Mohd Sadiq. Systematic review of software risk assessment and estimation models. *International Journal of Engineering and Advanced Technology*, 1:298, 2012.

[KP08] Barbara A Kitchenham and Shari L Pfleeger. Personal opinion surveys. In *Guide to Advanced Empirical Software Engineering*, pages 63–92. Springer, 2008.

[LH05] Steve Lipner and Michael Howard. The trustworthy computing security development lifecycle, microsoft corporation, 2005.

[McG05] Gary McGraw. Risk management framework (rmf). *Cigital, Inc*, 2005.

[McG06] Gary McGraw. *Software security: building security in*, volume 1. Addison-Wesley Professional, 2006.

[McG12] Gary McGraw. Software security. *Datenschutz und Datensicherheit-DuD*, 36(9):662–665, 2012.

[Mica] Microsoft. Benefits of the SDL. Available at https://www.microsoft.com/en-us/SDL/about/benefits.aspx, Last accessed: 2017-01-27.

[Micb] Microsoft. Evolution of the Microsoft SDL. Available at https://www.microsoft.com/en-us/SDL/resources/evolution.aspx, Last accessed: 2017-01-27.

[Micc] Microsoft. Microsoft Security Development Lifecycle Process. Available at https://www.microsoft.com/en-us/SDL/process/training.aspx, Last accessed: 2017-05-22.

[Micd] Microsoft. SDL for Agile. Available at https://www.microsoft.com/en-us/SDL/Discover/sdlagile.aspx, Last accessed: 2017-05-15.

[Mice] Microsoft. SDL for Agile Development - Introduction. Available at https://msdn.microsoft.com/en-us/library/windows/desktop/ee790617.aspx, Last accessed: 2017-04-25.

[Micf] Microsoft. SDL for Agile Development - Requirements. Available at https://msdn.microsoft.com/en-us/library/windows/desktop/ee790620.aspx, Last accessed: 2017-01-31.

[Micg] Microsoft. SDL Threat Modeling Tool. Available at https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx, Last accessed: 2017-04-26.

[MMW16] Gary McGraw, Sammy Migues, and Jacob West. BSIMM 7. Technical report, Building Security In Maturity Model, 2016.

[MN07] Michael D Myers and Michael Newman. The qualitative interview in IS research: Examining the craft. *Information and organization*, 17(1):2–26, 2007.

[Nor] Norsk senter for informasjonssikring NorSIS. Nasjonal sikkerhetsmåned. Available at https://sikkert.no/, Last accessed: 2017-05-03.

[NVD] NVD. National Vulnerability Database. Available at https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&cvss_version=3, Last accessed: 2016-11-02.

[Pel05] Thomas R Peltier. *Information security risk analysis*. CRC press, 2005.

[Pot09] Bruce Potter. Microsoft SDL threat modelling tool. *Network Security*, 2009(1):15–18, 2009.

[SA11] Ulrike Schultze and Michel Avital. Designing interviews to generate rich data for information systems research. *Information and Organization*, 21(1):1–16, 2011.

[Sch07] Thomas A Schwandt. *The Sage dictionary of qualitative inquiry*. Sage, 2007.

[Sil09] David Silverman. *Doing Qualitative Research*. SAGE, 2009.

Appendix A
Survey

Team

1. Hva er din rolle i prosjektet?

   – Stilling;_____

2. Har du jobbet med, eller har bakgrunn fra informasjonssikkerhet?

   ☐ Ja

   ☐ Nei

3. Hvor mange er dere i teamet som jobber på dette prosjektet?

   – Antall;_____

4. Har noen på teamet jobbet med, eller har bakgrunn fra informasjonssikkerhet?

   ☐ Ja

   ☐ Nei

5. **Hvis Ja:** Hvor mange?

   – Antall;_____

6. Har teamet blitt kurset i noen av disse sikkerhets treningsmetoder?

- ☐ Generell sikkerhets trening, gjennom kurs og kursmateriell
- ☐ Opptrening av eksperter
- ☐ Frivillig rolle-spesifikk sertifisering
- ☐ Obligatorisk rolle-spesifikk sertifisering
- ☐ Vi stoler på at tredjeparts utviklere holder seg oppdatert
- ☐ Nei

7. Hvilke av disse treningsmetodene tror du er mest effektiv?

- ☐ Generell sikkerhets trening, gjennom kurs og kursmateriell
- ☐ Opptrening av eksperter
- ☐ Frivillig rolle-spesifikk sertifisering
- ☐ Obligatorisk rolle-spesifikk sertifisering
- ☐ Vi stoler på at tredjeparts utviklere holder seg oppdatert
- ☐ Annen;_____

8. Har dere noen ansatte som er dedikert til å jobbe med informasjonssikkerhet?

- ☐ Ja, kun dedikert til informasjonssikkerhet
- ☐ Ja, men har andre ansvarsområder i tillegg
- ☐ Nei

9. Hva er sant for dette prosjektet?

- ☐ Produktet utvikles for in-house bruk
- ☐ Produktet utvikles for å selges
- ☐ Produktet utvikles for andre bedrifter, teamet er utleid til dem

10. Hvilken industri skal sluttproduktet brukes i?

- ☐ Finans

☐ Varehandel

☐ Produksjon

☐ Telekommunikasjon

☐ Teknologi

☐ Energi

☐ Transport og logistikk

☐ Medisin

☐ Annen;_____

11. Hvilken aldersgruppe tilhører de tiltenkte sluttbrukerne? *(Flere svaralternativer tillatt)*

☐ Alle

☐ Opp til 13 år

☐ 13 til 19 år

☐ 20 til 39 år

☐ 40 til 68 år

☐ Fra 68 år

☐ Vet ikke

Sikkerhet

12. Vil det ferdige prosjektet kreve en form for sikkerhet? *(F.eks: Personvernsbeskyttelse, kryptering, risiko overvåkning, osv)*

☐ Ja

☐ Nei

☐ Vet ikke

13. Hvor sikkert tror du sluttproduktet vil være?

- ☐ Svært sikkert
- ☐ Sikkert nok
- ☐ Sikkert til en viss grad
- ☐ Ikke sikkert
- ☐ Vet ikke

14. Hvor stor del av budsjettet brukes på sikkerhet?

- ☐ Under 1%
- ☐ 1%
- ☐ 2-5%
- ☐ 6-10%
- ☐ 11-15%
- ☐ Mer enn 15%
- ☐ Vet ikke

15. Hvilke retningslinjer/prosedyrer har dere dokumentert og godkjent for dette prosjektet? *(Flere svaralternativer tillatt)*

- ☐ Hendelser og respons planer
- ☐ Veikart for informasjonssikkerhet
- ☐ Kontinuitetsplaner
- ☐ Informasjonssikkerhet styringsstruktur
- ☐ Informasjonssikkerhetsstrategi
- ☐ Ingen
- ☐ Andre;_____

16. Hva tror du vil hjelpe å forsterke sikkerheten i prosjektet? *(Flere svaralternativer tillatt)*

- ☐ Avansert sikkerhetsteknologi
- ☐ Komiteer for IT styring
- ☐ Belønningssystem for de ansatte
- ☐ Bedre bevissthet for sikkerhet
- ☐ Øke antallet av de som dedikert jobber med sikkerhet
- ☐ Større budsjett
- ☐ Engasjement fra ledere
- ☐ Risiko analyser
- ☐ Annet;_____

17. Hvem tester sikkerheten i prosjektet?

- ☐ Vårt utviklerteam
- ☐ Internt sikkerhetsteam
- ☐ Eksternt sikkerhetsteam
- ☐ Kvalitetssikring
- ☐ Sikkerhets tilbydere
- ☐ Andre;_____

18. Utføres noen av de følgende metodene i prosjektet? *(Flere svaralternativer tillatt)*

- ☐ Penetrasjonstesting
- ☐ Code review
- ☐ Sikkerhets trening
- ☐ Identitet/Adgangskontroll
- ☐ Dynamisk analyse
- ☐ Statisk analyse
- ☐ Application firewalls/Virtual patching

- ☐ Trusselmodellering
- ☐ Andre;_____

19. Hvilke av de følgende metodene tror du gir best resultat med tanke på sikkerhet?

- ☐ Penetrasjonstesting
- ☐ Code review
- ☐ Sikkerhets trening
- ☐ Identitet/Adgangskontroll
- ☐ Dynamisk analyse
- ☐ Statisk analyse
- ☐ Application firewalls/Virtual patching
- ☐ Trusselmodellering

Risikoanalyse

20. Hvordan er risiko overvåket og håndtert i prosjektet nå?

– _____

21. I prosjektet, hva tror du kan skape risiko? *(Flere svaralternativer tillatt)*

- ☐ Mangel på personell
- ☐ Urealistiske tidsplaner og/eller budsjett
- ☐ Utvikling av feil funksjoner
- ☐ Utvikling av feil bruker grensesnitt
- ☐ Flere forandringer i prosjekt kravene
- ☐ Mangel på eksterne komponenter
- ☐ Eksterne komponenter
- ☐ Utvikling går for tregt eller for fort

☐ Mangel på tester og validering

☐ Komplekse systemer

☐ Annet;_____

22. Har du hørt om noen av de følgende metodene/studiene? *(Flere svaralternativer tillatt)*

☐ BSIMM

☐ OpenSAMM

☐ Microsoft SDL

☐ SDL Agile

☐ Cigital Touchpoints

☐ ISO 27000

☐ OWASP top 10

☐ CERT Secure Coding Standard

☐ Nei

23. Har du hørt om noen metoder/studier ikke listet i spørsmål 22?

☐ Ja;_____

☐ Nei

24. Har dere en rådgivende gruppe som kan hjelpe med risikohåndteringsprosessen eller sikkerhetsaspekter i prosjektet?

☐ Ja, kun til risikohåndteringsprosessen

☐ Ja, kun til sikkerhetsaspekter

☐ Ja, har begge deler tilgjengelig

☐ Nei

25. Jobbes det med risikoanalyser for informasjonssikkerheten i prosjektet?

☐ Ja *(Vennligst fortsett fra spørsmål 25.2)*

☐ Nei *(Vennligst svar på 25.1)*

Hvis Nei:

25.1. Hvorfor ikke? *(Flere svaralternativer tillatt)*

☐ Mangel på tid

☐ Mangel på budsjett

☐ Mangel på kunskap

☐ Mangel på verktøy

☐ Ser ikke poenget

☐ Har ikke tenkt på det

☐ Annen grunn;_____

Hvis Ja:

25.2. Har det oppstått vanskeligheter ved å utføre risikoanalyser? *(Flere svaralternativer tillatt)*

☐ Ja, ikke nok ressurser i budsjettet

☐ Ja, ikke nok tid

☐ Ja, har ikke nødvendige verktøy

☐ Ja, ikke nok kunskap

☐ Andre vanskeligheter;_____

☐ Nei

25.3. Hvem er inkludert i å finne løsninger til risikoene i prosjektet?

☐ Prosjektleder

☐ Utvikler

☐ Designer

☐ Andre;_____

25.4. Hvor ofte evalueres risikoen som er tilstede i prosjektet på ny?

☐ Daglig

☐ Ukentlig

☐ Månedtlig

☐ Når det passer

☐ Risikoen evaluates ikke på nytt

25.5. Hvordan dokumenteres risikoen funnet?

☐ I en risiko kunnskapsbase

☐ I en risiko database

☐ Dokumenteres ikke

☐ Andre metoder;_____

25.5.1 Hvilken informasjon dokumenteres? *(Flere svaralternativer tillatt)*

☐ Historiske data

☐ Statistiske data

☐ Rapporter

☐ Tips og anbefalingen om hvordan risikoen håndteres

☐ Sammenligninger av risikoer.

☐ Annet;_____

Appendix B
Interview Guide

Prosjektet

1. Kan du fortelle litt om hva du jobber med til daglig?

2. Kan du fortelle litt om prosjektet du jobber med nå?
   — Produkt til eget bruk eller salg? Utleid team
   — For hvilken industri?

Team

3. Kan du fortelle litt om teamet du jobber med i dette prosjektet?
   — Hvor mange er dere?
   — Hvilken bakgrunn har dere?

4. I teamet, har dere fokus på informasjonssikkerhet?

5. Blir det gitt opplæring innen sikkerhet?
   — Hvorfor / Hvorfor ikke?
   — Tror du det er viktig med mer sikkerhetsopplæring?

Sikkerhet

6. Hvordan jobber dere med sikkerhetsaspekter i prosjektet?
   — Bruker dere noen spesielle prosesser, modeller, etc.

7. Har dere noen som spesifikt jobber opp mot sikkerhetsaspektet?

8. Hvordan tester dere sikkerheten underveis?
   — Hvem tester?

9. Hvordan vet dere hva som skal sikres i prosjektet?

10. Syns du dere jobber nok opp mot sikkerheten i prosjektet?
    — Hvorfor / Hvorfor ikke?

Risiko

12. I ditt prosjekt, hva tror du skaper risiko?

13. Har dere gjort risikoanalyser for prosjektet?
    — Hvorfor / Hvorfor ikke?

14. Føler du at dere er rustet til å håndtere sikkerhetsangrep?
    — Hvorfor / Hvorfor ikke?

15. Har dere planer for hvordan dere håndterer sikkerhetsbrudd?

Resultater

16. Hva er dine tanker om risikoanalyser?

Bruk av risikoanalyse

17. Tror du risikoanalysen hjalp, med tanke på sikkerheten?

Ingen bruk av risikoanalyse

17. Tror du en risiko analyse ville hjulpet, med tanke på sikkerheten?

18. Ønsker du at det ble utført risikoanalyser i prosjektet?
    — Hvorfor ikke?

Appendix C
Answers from Interviews

Following are the answers from the eight interviews held during this project. All the interviews are given in Norwegian as this was the language the interviews were conducted in. Details for the interviews can be found in Table C.1, details include if the interview was held on the platform Skype of in person, who the interviewer was, the role of the interviewee, and how long the interview lasted. All the interviews in this appendix are rendered from recordings done by a tape recorder. All the interviewees consented to being recorded. To some extent the interviews have been altered in order to keep the anonymity of the interviewee and their organisation. The meanings and justifications of their answers are still the same, as the only thing altered were naves of companies and customers. Some questions and answers are omitted as the nature of the answer would conflict with the interviewees or their organisations anonymity.

	Skype or in-person	Interviewer	Role of interviewee	Interview time
Interview 1	Skype	Heidi Svendsen	Product owner	20 minutes
Interview 2	Skype	Heidi Svendsen	Project leader	18 minutes
Interview 3	Skype	Heidi Svendsen	Development leader	13 minutes
Interview 4	In-person	Heidi Svendsen	Consultant and software developer	20 minutes
Interview 5	Skype	Heidi Svendsen	Software developer	15 minutes
Interview 6	Skype	Heidi Svendsen	Team leader and software developer	18 minutes
Interview 7	In-person	Heidi Svendsen	Technical project leader	18 minutes
Interview 8	In-person	Heidi Svendsen	Position in the security group	38 minutes

Table C.1: Details of the interviews conducted.

C.1 Interview 1

1. Hva jobber du med daglig? Hvilket prosjektet jobber du med?
   - Jeg holder på med et kontinuerlig prosjekt, vi lager et produkt som håndterer innkjøp, lagerstyring, produksjonsstyring, alt som har med materialflyt å gjøre. Et standard system som selges ut til kunder innenfor alle mulige bransjer. Så dette er noe som blir lagd i releaser tre eller fire ganger i året.
2. Så da er det et prosjekt som er mest for logestikk?
   - Ja, logistikk og supply-chain er der vi har fokus.
3. Blir produktet solgt til alle som ønsker den tjenesten?
   - Ja, det kan du si. Vi selger jo et produkt som i sin nåværende form er on-premis, det vil si at det installeres ute hos kunden på en eller annen måte. Kunden er ansvarlig for drift og bruk av applikasjonen. Det er alt fra små kunder, minste er vel 2 personer, til store organisasjoner, 10-12 tusen brukere.
4. Hvor mange er dere som jobber med dette til daglig?
   - Jeg har 5 utviklere, og 15 konsulenter, pluss et support apparat og selgere.

5. Har du noen som jobber sikkerhet?

   – Nei, vi er ikke så opptatt av det, vi har vertfall ikke vært. Det er egentlig noe vi ikke har hatt så mye fokus på. Noe av grunnen til det er at det ikke er vi som er ansvarlig for sikkerheten. Det er kunden som installerer dette her i sitt miljø og bruker det der. Som da passer på hvordan det blir håndtert med tanke på brannmur og hvilke personer som har tilgang, hva du får gjøre og ikke gjøre.

6. Da har du ingenting med access-controll og slike ting, før dere installerer hos kunden?

   – Nei, altså kunden kjøper applikasjonen og installerer den hos seg. Det kunden som setter seg ned, med oss selvfølgelig, og finner ut hvilke personer som skal ha tilgang til hvilke funksjoner og hvilke muligheter de skal få lov til å gjøre i systemet. Så det vi tilbyr er en funksjonalitet hvor du kan mappe brukere og brukergrupper opp mot funksjoner. Skal du få lov til å se, skal du få lov til å registrere salgsordre, skal du få lov å refakturere, skal du få lov å registrere en ny kunde, skal du få se på kunden eller skal du få lov til å endre på den også? Men det er noe kunden må bestemme seg for, når han tar applikasjonen i bruk hvilke begrensninger han vil gi.

7. Har dere utviklet hvilke begrensninger det går ann å gi?

   – Ja, det har vi laget selv. Det er en mapping mellom hver funksjon, type registrering av kunde, leverandør, innkjøpsordre, artikkelregister, det er jo tusentals slike funksjoner. Ihvertfall tusen sikkert. Og så kan brukeren velg om han da skal gi tilgang ned på funksjonsnivå. Om han i den funksjonen skal få lov til å oppdatere eller bare se. Så kan han si at dette skal være for enkelt brukere eller at de skal grupperes i en eller annen form for gruppering, brukertype, kategori, litt avhengig. Det er litt forskjellig, har du 5 brukere så grupperer du ikke de, men har du 10000 så gjør vi noe med det.

8. Har dere sett på hvilke feil som kan skje i forhold til dette? Hvis noen for eksempel får tilgang til plasser de ikke skulle hatt tilgang.

   – Tja, det er det jo selvfølgelig. Du kan jo alltid gjøre feil, altså brukeren sletter ting han ikke burde og slike ting. Så har vi jo noen som er litt opptatt av at noen ikke skal lure de. Altså at de ikke skal drive underslag, slik at vi har funksjonalitet som gjør at du ikke kan slette en transaksjon. Du har lov til å kansellere den, selvfølgelig, hvis kunden angret seg, men du får ikke slettet det, så det vil ligge igjen et spor der. Også dette er ting som kunden er ansvarlig for å sette opp eller ikke. Vi har hatt noen gjennomganger, men vi har noen kunder som har amerikanske eiere, og

de er jo opptatt av aktiviteter. Så ved å sette opp applikasjonen på en bestemt måte tilfredsstiller vi krav der også. For da er det sporing og at ikke du får lov til å slette en innkjøpsordre, får ikke slette en faktura, hvis du gjør noe så er det logget bakover i systemet for å finne ut hvem som har gjort hva.

9. For da er du litt inne på sikkerhet i selve applikasjonen.

   – Ja, vi har kanskje hatt mer fokus på å spore hva som har skjedd. Enn å begrense hva som skjer. Men der er det et veldig forskjell på norske kunder og f.eks. engelske og amerikanske kunder. Norske bedrifter er mye mer åpne, du er ansatt der fordi du er en person som de har tillit til. Og norske bedrifter er ikke så store, så det er ikke slik at du har en mann som gjør en ting, veldig mange gjør forskjellige ting så de har normalt tilgang til det meste. Det er veldig få, i alle fall i vår erfaring som velger å sette begrensning på hva en bruker får lov til. Du setter kanskje det på, hvis du er i en produksjonsbedrift, så vil du sette begrensninger på de som er ute i produksjonslokalene, de får "lov" til å registrere om de har produsert noe, om de har brukt tid og slikt. De er på en måte ikke inne å oppretter kunder. Når du kommer litt opp på et administrativt nivå, så er det ofte slik at alle har tilgang til alt. Selv med vårt selskap, jeg har egentlig ikke så mye inn i økonomisystemet å gjøre, men kunden ringer meg hvis en faktura har stoppet opp. Da har jeg tilgang til økonomisystemet for å se, jeg kan jo ikke sende den videre til en eller annen som sitter et annet sted som skal se på noe. Det er på en måte tradisjonelt litt åpent. I følge det vi kan få selvfølgelig, fordi noen gjør en feil, mange er jo opptatt av at du heller får spore hva som har skjedd, og begrense på forhånd.

10. Har dere satt opp modeller på hvordan brukeren kan gjøre feil når de bruker systemet?

    – Nei.

11. Så dere setter det bare opp ettersom det kommer problemer på veien?

    – Som regel blir det for vår applikasjon gjort slik at alle har tilgang til alt, så blir det satt begrensninger for noen. Men, ja hvilke feil som kan skje er jo nesten helt umulig å vite. Vi har ikke brukt noe mye tid på å tenke ut det rett og slett.

12. Kunne du sett om det hadde hatt noe mer verdi å sett på det?

    – Jeg tror ikke vi hadde gjort det nei. Dels fordi kundemassen er såpass spredd fra 2 brukere til 10 000. Fokuset hos dem veldig forskjellig. For de 10 000 er det ofte noen som skal ut å bestille noe, mens de som er

administrative brukerne har jo tilgang til alt. De som er ute gjør bare det de må for å bestille varer og levere inn til bedriften. Nei, så egentlig ikke. Det er ikke så veldig mange som er opptatt av det egentlig.

13. Når en kunde ringer å sier at det har oppstått en feil, hvordan håndterer dere det?

    - Hadde de kontaktet support hos oss så logger vi oss rett på for å finne ut hva som har skjedd. Da ligger det jo sporinger i systemet som regel, over hvem som har gjort hva og hvem som har gjort hvilke transaksjoner. Som regel sporer vi bare hvem som har endret en kunde, ikke hva som er endret. Men, i og med at noen er litt mer opptatt av sikkerhet enn andre, så har vi sporing på noen enkelt felter, f.eks hvem som har endret bankkontonr. For å sikre at ikke noen har endret bankkontonr ditt når kunden betaler, slik at pengene kommer et annet sted. Men det er unntaksvis, kun enkelte ting hvor det er blitt utført på. Kunden må aktivere sporing, hvem som har gjort endringer.
    - Den sikkerheten vi har er et passord regime, at du må logge inn med et passord. Dette er den eneste sikkerheten som vi har inne i systemet by default. Kunden kan bestemme policy på passord selv.

14. Hvorfor bruker du ikke risikoanalyser?

    - Siden det ikke er vår applikasjon. Hadde vi laget applikasjonen til eget bruk, så hadde vi vært mer opptatt av det. Men her er det kunden som er ansvarlig for å gi tilgang, kryptere databasene sine, sette begrensninger, altså det er det ikke vi som programvareleverandør som tar ansvaret for eller som har ansvaret for. Litt som personvern. Det er jo kunden som velger å bruke det slik. Han må på en måte gjøre den risikovurderingen selv.

C.2 Interview 2

1. Hva jobber du med?

    - Jeg har vært hos bedriften i nesten 6 måneder, det betyr at man nermest er en veteran. Vi er veldig store i utvikling hos bedriften. Min stilling er prosjektleder, jeg har jobbet på tre ulike prosjekter. De har vært i forhold til å implementere løsningene av de produktene som vi har. To av de hadde hatt våre produkter på deres plattform fra før.

2. Kan du fortelle litt om hva du jobber med akkurat nå?

   - De kundene jeg jobber med nå har aldri hatt noe med broadkasting å gjøre. Det jeg jobber med dem er å lage et vedlikeholdssystem. Når du er prosjektleder her, så går det veldig mye på å koordinere i og med at vi er på forskjellige steder. Mye går på vedlikeholdelse, og mye går på de vil se på utskiftning av selve infrastrukturen hos dem. Det krever selvfølgelig en stor forandring. For å være spesifikk så må vi skifte, omskrive og videreutvikle på vår nåværende infrastruktur. Det er på det ene prosjektet.
   - Den andre som jeg er i, er akkurat lansert. Der går det mye ut på å håndtere trafikken som kommer til å skje når folk er inne å ser på sendingen, og hvordan det kommer til å gå på vår platform.

3. Hvor mange er dere som pleier å jobbe på disse prosjektene?

   - Optimalt, la oss si vi har en kunde som aldri har brukt vår platform, da vil det vanligvis være en teknisk, en teamleader, en teknisk account manager, en selger, en løsnings arkitekt, og en prosjektleder. Gjerne 4-5 personer, som utelukkende skal håndtere prosjektet. Når det kommer til utvikling er det veldig forskjellig, vi har tre forskjellige avdelinger som gjør hver deres oppgaver. Derfor kan jeg ikke si spesifikt om det er en person, eller ti som jobber.

4. Har dere noen som jobber direkte mot sikkerhet på prosjektene deres?

   - Ja, altså vi har en sikkerhetsansvarlig i bedriften, han er ansvarlig for alt som har med sikkerhet å gjøre. Både internt og eksternt. Det blir supplert, selvfølgelig, med erfaring fra den teknisk kyndige personen som har langsert platformen. Akkurat nå sitter de som leverer våre prosjekter hos noen eksperter som har vært med fra starten. De er alt mulig, og våre guruer som tenker på sikkerhet veldig veldig mye.

5. Gir dere opplæring til de tekniske ansatte innen sikkerhet?

   - Nei. Vi gir opplæring på hele vår platform og vi gir opplæring helt fra starten når du skal begynne å levere. Vi leverer jo backend delen, og opplærer alt som har med den delen å gjøre. Men når det kommer til hva som blir endret på de ulike tingene, blir det gjort forskjellig hos våre kunder. Når det kommer til sikkerheten her, er det noe vi er veldig interesserte i, men også litt utenfor våre hender.

6. Hva gjør dere og hvordan jobber dere med sikkerheten på backend?

   - Det er lovgitt hva vi skal gjøre når det kommer til rent sikkerhetsmessig og rent oppbevaringsmessig. Vi sørger for at det holdes up to date. Det gjør vi med at folk blir sendt på kurs, og folk blir sendt på workshops. Vi holder oss informert og sørger for at våre systemer er helt under korrekt nivå.

Vi leverer også en betalings løsning som ble utviklet av våre partnere. Der har vi ingenting som blir lagret hos oss. Vi slipper unna en del sikkerhetssertifiseringer fordi det ikke vi som har med sikkerheten å gjøre i denne. Vi gjør selve integrasjonen, men det er andre som er mye bedre, mye flinkere til betalingsbiten som tar seg av dette. Så det går veldig mye på å jobbe med sikkerhet som tech kyndig hos våre partnere, og tredjeparts venders som vi har. De må holde seg up-to date med det tenker vi.

7. Når dere integrerer løsningen deres hos kunden, tester dere sikkerheten eller er det kunden som står for det?

   – Det er litt forskjellig. Det avhenger veldig mye på kunden. Noen kunder har små behov, da klarer de veldig mye selv. Noen kunder, som har vår løsning for første gang, blir introdusert til det hele, og vi står for det hele. Felles er at sikkerhetblir testet selvfølgelig, så mye som over hodet mulig.

8. Vet de som jobber med sikkerheten hvilke trusler de står ovenfor i prosjektene sine?

   – Nei ikke spesifikt. De står jo ovenfor f.eks. innholdet som blir sikret hos oss er noe som er sikkerhetsrelatert. Det er noe vi jobber med veldig mye. Kryptering er noe som vi leverer og vi må forholde oss til. Vi har ulike verktøy til å gjøre det, men har et egetutviklet verktøy for å gjøre disse tingene. Vi har vår video team, som er på høyeste plan innenfor det. Det kan være noe som de jobber med innenfor sikkerhet. Jeg tør ikke svare med spesifikt på de andre tingene.

9. Du sa dere hadde flere risikomodeller.

   – Ja, altså, jeg brukte ganske mye tid på skolen til å definere forskjellige former for risikomodeller, og hvordan man bruker de. Og så ser jeg når jeg kom ut i arbeid, at mye av det er fullstendig irrelevant. Som det ofte er med mange ting. Det hender man må tilpasse risikomodellen for hver kunde. Det er noen som fungerer, noen kunder har du f.eks. et ukentlig møte med, som er veldig spesifikt og definert. Du har da veldig kontroll over hva man går gjennom og du gjør det på en slik måte at er lett å forholde seg til. For slike kunder er det veldig lett å implementere en sikkerhetsrisikomatrise. Som du holder oppdatert og som du veldig aktivt bruker. Samtidig så har du kunder hvor du må reagere fra en dag til en annen. Nermest fra en time til en annen, veldig uforutsigbar, veldig dynamisk. Å prøve å opprettholde en sikkerhetsmatrise er fulstendig irrelevant fordi de risikoene du kommer på har fort endret seg på noen timer kanskje. Så det er ikke en risikomodell som i seg selv er enkel å

opprettholde. Det er en risiko i seg selv at du ikke har tid til å opprettholde en kontrollert risiko analyse, og da må du forholde deg til det. Men det som vi bruker aller mest er den klassiske, og du kan bruke hvilke verktøy du vil. Vi bruker Puls som er veldig intuitivt og veldig visuelt. Det har jeg funnet ut at er det viktigste hos en kunde, altså at det er visuelt. Du har en risk score og en impact som du setter inn i den enkle risikoen. Du bruker litt tid på å planlegge og komme frem til den. Basert på hva du vurderer så har du en handlingsplan.

10. Ser du noen fordeler og ulemper med bruk eller ikke bruk av risiko analyser?

    – Fordelen med å bruke den er stor når det gir mening og kunden er tydelig, da kan du se en kjempe fordel med at du er forberedt. Det gir deg mulighet for å lage en plan B og en plan C. Den absolutt den største fordelen er å ha en veldefinert handlingsplan på hva som kommer til å skje, og samtidig ha en oversikt over hva du forventer kommer til å skje. Ulempen med det er at det krever mye jobb, det er at du skandaliserer og vedlikeholder det på et vis. Hvis du ikke vedlikeholder den, bare en gang, så kan du glemme den, da har det endret seg for mye. Du må gjøre et forarbeide først, hva kommer jeg til å gjøre, hvordan utspiller dette prosjektet seg. Er det muligheter for å bruke en enkel matrise?
    – Fordelen med å ikke bruke den er at du tvinger deg selv til å være veldig fleksibel, og reaktiv på enkelte problemer. Du tvinger deg selv til å forstå at du kommer til å ta beslutninger som høyst sannsynlig kommer til å være feil veldig mange ganger, men likevel så står du fast i den beslutning og ikke ut fra det. Det gjør at du har en stabil/flytende tidsplan som fortsetter. Du slipper å stoppe opp å sjekke matrisen din hver gang det skjer noe. En matrise kan også forhindre deg i å treffe en beslutning fordi du er redd for at det kan være en feil til slutt. Ulempen vil selvfølgelig være alt dynamisk, at du ikke kommer til å kontrollsikre ting, som er forventet av deg, spesielt som en prosjektleder. Og du kommer ikke til å kunne gjøre alt som er korrekt, som i prinsippet også er en form for forventning. Så det går litt på erfaring, det går litt på personlighetstype.
    – Legg vekt på at det ikke er så mye om å bruke eller ikke å bruke, men å definere hvordan du har tenkt å løse problemer når det kommer til risiko.

11. Føler du at dere er rustet til å håndtere sikkerhetsangrep som skjer, eller er det kunden som håndterer det?

    – Bedriften er, jeg er ikke for å si det slik. Hele bedriftens egenskaper og kunnskaper kan en lene seg på, så det er veldig enkelt å springe i det. Det er en bedrift som har en kultur å dele viten som ingenting og som har en kultur som prøver å hjelpe hverandre om utfordringene, om de er

sikkerhetsrelaterte eller om de er risiko eller om det er utvikling/teknisk, så spiller det ingen rolle fordi kulturen går på å dele. Den største trusselen for sikkerheten er den menneskelige feil, derfor er det viktig å stå sammen om problemene. Du kan ikke ta høyde for en menneskelig feil.

C.3 Interview 3

1. Hva jobber du med, og hva er bakgrunnen din?
   - Ja, jeg jobber med utviklingsprosjekter i bedriften. Jeg jobber for tiden som noe vi kaller utviklingsleder, så jeg koordinerer litt de forskjellige tingene vi driver med her. Bakgrunnen er at jeg har gått ut fra NTNU for noen år siden også har jeg jobbet i denne bedriften siden oppstarten.
2. Hvor mange er dere som pleier å jobbe på prosjektene?
   - Ja, det er jo litt variernede. Vi leier inn en del konsulenter og vi har en del fast ansatte, så vi er vel en 8-10 fast ansatte og så har vi mellom 10-5 innleide konsulenter hos oss. Det varierer litt, med tanke på finansiering og slikt.
3. Har dere en del fokus på sikkerhet?
   - Våre løsninger er sikkerhetsløsninger, så det er klart at vi alltid har hatt en del fokus på det.
4. De som jobber med sikkerhet, er det rene utviklere eller sikkerhetsutviklere?
   - Det er rene utviklere sånn sett, med litt varierende kompetanse og interesse for sikkerhet. Men det er klart, hvor lenge og mer man jobber med dette her ser man lettere viktigheten med sikkerhet.
5. Gir dere sikkerhetskursing til deres ansatte?
   - Det er ikke så mye direkte kursing, det er ikke det. Vi har litt introduksjon, og slike ting. Dermed lærer man litt etterhvert stort sett.
6. Bruker dere noen spesielle modeller innen sikkerhet? F.eks. SDL.
   - Nja, litt. Vi har i alle fall prøvd å lage noen prosesser som til en viss grad er inspirert av SDL. Men det er nok litt på begynnerstadiet fremdeles.
7. Blir det slik at sikkerheten kommer i tillegg til det dere utvikler først?
   - Nei, det vil jeg ikke si. Vi tenker på sikkerhet gjennom hele prosessen, altså fra vi begynner å analysere problemstillingen. Det er nok ikke slik at sikkerheten kommer etterpå, det er med hele veien.

8. Tester dere underveis? Hvilke sikkerhetsaspekter er dere mest interesserte i å teste?

   – Det kommer litt ann på prosjektet. En god del av det er ganske standard web applikasjoner, og da blir det de standard sårbarhetene som finnes i web applikasjoner. F.eks OWASP Top 10 og slike ting. For litt andre bruksområder, så blir det jo hvilken grad av sikkerhet en skal gjøre på transport nivå og meldings nivå og slikt. Kryptering og signering, så det er ofte en diskusjon på hvilket nivå en skal legge seg på.

9. Er det bare web applikasjoner dere driver med? Dere har ikke begynt å se på applikasjoner for mobile enheter?

   – Nei, det har vi egentlig ikke. Altså vi har ikke kommet dit at vi har noen apps som er i bruk.

10. Tester dere selv, eller leier dere inn konsulenter til å teste?

    – Begge deler. Altså vi har innleide, eksterne konsulenter i tilleg til at vi gjør ting selv.

11. Mener du dere jobber nok opp mot sikkerheten?

    – Om det jobbes nok ja. Altså jeg vil nå si at vi har fokus på det hele tiden så. Innenfor akkurat det jeg driver med så vil jeg si at vi har et bra fokus på sikkerhet, vil jeg si.

12. Har dere satt opp hvilke trusler dere er mest utsatt for?

    – Ja, vi har ikke gjort noen ROS analyse, det ligger litt ved siden av utvikling. Det er med folk fra utvikling når vi gjør slikt, men det er ofte litt på siden av. Slik som jeg opplever det i alle fall.

13. Utenom denne ROS-analysen, har dere noen risiko analyser som går direkte mot utvikling?

    – Nei, altså vi driver vel ikke med trusselmodellering og slik egentlig.

14. Hvorfor ikke?

    – Nei, vi gjør ikke trusselmodelleringer, vi gjør ikke det.

15. Hva tenker du rundt å gjøre en eventuell risikoanalyse?

    – Vi gjør det jo på et eller annet nivå, altså vi har jo risiko sannsynlighet-snivåene men ikke direkte inn mot utviklingsprosjektene. Det ligger litt ved siden av. Kanskje det er litt dumt, men hvordan vi skal løse det har ikke jeg noe godt svar på akkurat nå. Jeg tror vi kunne hatt nytte av en risikovurdering om vi hadde hatt bedre kunnskap og resurser satt av til det.

C.4 Interview 4

1. Hva jobber du med? Hva er bakgrunnen din?

   – Jeg jobber med systemutvikling, og så er jeg konsulent. Jeg er utleid til kunder, men ikke så mange kunder. Jeg har vært i flere år hos en kunde og nå er jeg utleid til en annen. Der jeg er nå er sikkerhet veldig viktig. Da jeg svarte på spørreundersøkelsen din, svarte jeg med bakgrunn på mitt forrige oppdrag. Der var jeg med på å lage et system fra bunnen av.

2. Hvor mange pleirer dere å være på teamene hos kunden?

   – Det varierer veldig, men de fleste er fra 2-3 til kanskje 6-7-8. Akkurat nå er det 6 programmerere, jeg er også teamleder, og programmerer ikke så mye lengre.

3. Er det kun rene utviklere med, eller har dere sikkerhetsutviklere i tillegg?

   – Det er rene utviklere som er på teamet. Men på mitt forrige prosjekt så leide vi inn noen eksperter på sikkerhet i en kort periode, akkurat når vi startet.

4. Jobber dere noe mer med sikkerhet utenom det som trengs under utviklingen?

   – Ikke spesielt, vi jobber jo med å ha en viss sikkerhet på innlogging og slikt. Vi laget et API og hadde en viss sikkerhet for å kunne aksessere det da. Men jeg vil ikke si at vi har noen stor fokus på det.

5. Så dere på hvilke sikkerhetshull som eventuelt kan oppstå?

   – Ja, når vi hadde inne de to konsulentene så forklarte jo de en del om slikt. Da evaluerte vi faktisk risikoen. Vi kom egentlig frem til at det systemet der ikke var høy kritisk. Vi tilpasset dermed litt i forhold til det da.

6. Har dere noe opplæring i sikkerhet for utviklerne i din bedrift?

   – Nei. Vi har opplæring i det konsulentene ønsker opplæring i. Vi går på de kursene, og de konferansene vi vil. Så det er klart at av og til så er jo sikkerhet et tema på konferanser, men det er ikke slik at vi gjennomfører noen spesiell opplæring innen sikkerhet hos oss nei.

7. Da dere drev på med innloggingen, og sikkerheten der. Testet dere noe da?

   – Ja, vi testet jo litt.

8. Testet dere selv da?

- Vi hadde ikke eksterne inne til å teste. Jeg vet at vurderte å ha noen inne, men jeg tror ikke det ble gjort.

9. Det prosjektet, var det da kun innlogging, eller lagde dere nettsider rundt også?

   - Det var to prosjekter på en måte. På API biten så var det nøkkelbasert, hadde du den nøkkelen, så slapp du inn i systemet. Der var det ikke noe brukergrensesnitt, du aksesserte via andre verktøy. På det andre var det litt brukergrensesnitt, der var det et helt annet innloggingsmiddel. Vi lagde kun innloggingen.

10. Vet du hva som skapte risiko i dette systemet?

    - Den som koder, skaper jo risiko med koden sin. Og du kan jo da plutselig risikere at du kan aksesser data uten å være innlogget.
    - Miljøet der systemet kjører, der kan det selvfølgelig være forskjellige typer risiko. En ting er jo inntrengning. Nå kjørte vi alt i skytjenester og da tenkte vi at det er viktig at de som driver skyen har god sikkerhet, og gjør det sannsynligvis bedre enn det vi gjør.
    - Så er det også sikkerhet når det kommer til nedetiden til systemet. Nå var ikke dette et veldig oppekritisk system, så vi var ikke så veldig bekymret for det. Og derfor var det godt nok i massevis. Men det var nå med på å skape en risiko i alle fall.

11. Den skyen dere brukte, var det kunden sin eller en tredjepart?

    - En tredjepart.

12. Ble tjenesten du utviklet integrert med kundens andre tjenester?

    - Ja, det var litt integrasjon med deres tjenester ja. Alt fokuset på sikkerhet og ansvar lå hos kunden, jeg var kun innleid til dem. Derfor hadde jeg ikke noe ansvar for systemet, jeg var kun innleid som en resurs.

13. Hvis noen hadde angrepet systemet, føler du systemet var rustet til å forhindre at de kom seg inn?

    - Noen typer angrep hadde angriperne kommet seg inn med. F.eks hvis de hadde klart å få tak i nøklene til de som hadde de, da ville de kommet seg inn. Men med generelle angrep, så ville det vært mye vanskeligere å få tilgang.

14. Hadde dere handlingsplaner i tilfelle angripere kom seg inn i systemet?

    - Vi hadde ingen planer for det. Det var også fordi det ikke var så kritisk.

15. Kjenner du til noen risikomodeller som brukes i utvikling?

- Det snakket jo de konsulentene som var inne hos oss en del om. Så vi var jo gjennom noe av det.

16. Har du noen tanker om disse prosessene?

    - Av det jeg husker, så var det jo mye nyttig i disse verktøyene, som man kan bruke når en har behov for det.

17. Tror du du kunne kommet til å begynne å bruke slike metoder?

    - Jo, neei, jeg tror ikke det. Klart hvis jeg hadde hatt behov og satt meg inn i det så hadde jge kanskje brukt de, men det er jo greit å ha eksperter til det hvis man har behovet.

C.5 Interview 5

1. Hva jobber du med?

    - Jobber som softwareutvikler. Jobber litt med skytjenester og en god del med apps som kobler seg til forskjellige typer hardware som vi har her via blåtann. Jeg lager alt mulig av software for å få dette til å virke, alt fra å transportere data fra et fysisk instrument som vi har stående hos hos kundene og så opp i skyen. Det er kortfattet det jeg driver med. Det innebærer også mye med sikkerhet da, hvordan kan vi beskytte dataen fra instrumentene opp til skyen. Og hvordan kan vi sikre at folk ikke stikker av med dataen.

2. Hvor store team pleier dere å jobbe i? Hvor stor er teamet du jobber i nå?

    - Vi er jo et ganske lite firma. Vi er 5 på utviklingsavdelingen, og det er egentlig det teamet vi jobber med hele tiden. Men vi er to stykker som driver med apps opp til sky. Og så har vi jo konsulenter inne hele tiden, så det varierer veldig, alt fra 2 – 5.

3. Har noen av dere jobbet med sikkerhet opp mot produktene?

    - Vi kommer jo bort i det i det vi gjør. Men ingen av oss har den stillingen hvis det var det du lurte på.

4. Får dere noe opplæring innenfor sikkerhet?

    - Det er veldig lite opplæring. Det er slik at vi lærer mens man jobber med det. Vi har økt antall ansatte veldig mye det siste året, så det går veldig for i svingene her.

5. Kan du snakke litt om sikkerhetsaspektene med det dere jobber med nå?

- Det er mye når det kommer til sikkerhet da. Vi har jo mange deler av det da, men vi har på en måte våre egne ting da, for å si det slik. Egne patenter, og hvordan vi beskytter de, er jo en ting. Men du tenker kanskje på brukerdata og det?
- Det har vi ikke tenkt nok på da. Vi bruker en tredjepart for å håndtere brukerdata, og da også, egentlig alt vi har da. Vi har da en avtale som sikrer oss at vi har lov til det da, med EU reglene. Det skal jo være sikkert da, men vi stoler veldig mye på tredjeparten når det kommer til sikkerhet, og at de holder dataene sikret. Det er de som står for kryptering og behandling, egentlig alt det der. Og tilgang til det styrer vi gjennom våre nøkler og passord. Der sitter noen få av oss med nøkler til dataserveren, så da gir vi litt mindre rettigheter til konsulenter som er inne hos oss. Ut mot omverden så er det beskyttet slik at brukeren må være logget inn for å få tilgang til dette her. Men hvis du først er logget inn, så har du tilgang til veldig mye da. Men vi lagrer veldig lite sensitiv informasjon da, så det er jo ikke så mye. Det er ikke telefonnummer en gang, det er bare navn og e-post. Det ser vi på som ganske lav risiko. Men vi har ikke noe fancy system for noe av dette, vi gjør som vår tredjepart anbefaler og så har det gått bra hittil i alle fall.

6. Tester dere denne sikkerheten?
   - Nei. Vi har mange ting på planen, men ting tar tid.
7. Hvilke data lagres av hardwaren deres?
   - Bittelitt brukerdata og så forskjellige måledata fra miljøet utstyret er satt i. Og vi lagrer lokasjon på utstyret slik at du kan lage et slags kart over disse måledataene.
8. Har dere sett på mulighetene for at folk som ikke skal ha tilgang kan komme inn å endre på måledataene?
   - Det er sikkert mulig hvis en vil, men nei vi har ikke undersøkt det i noen stor grad. Utover at det er beskyttet med passord og slik så er ikke.
9. Har dere sett noe på risikoen om hva som kan hentes, og stjeles, fra utstyret deres?
   - Jeg har ikke gjort det. Jeg tror ikke noen andre har gjort det heller. I grove trekk så har vi sagt det slik at vi ikke tror at denne informasjonen er kritisk på noen som helst måte. Den dataen vi henter ut er veldig viktig for brukerne som har utstyret i deres hus, for å finne ut om det er trygt å bo der eller ikke. Men det har ikke så mye verdi for alle andre. Så sånn

sett så er det jo en liten risiko for at det skal bli borte da, men vi har ikke gjort noen grundig risikoanalyse.

10. Har dere noen sikkerhetsgrupper som av og til er inne å ser på softwaren deres?

    – Ikke direkte knyttet til sikkerhet, men vi har jo konsulenter inne som har jobbet med skytjenester før som har hjulpet oss med å sette opp grunnleggende sikkerhet. De har da i stor grad kommet med anbefalinger på hva vi bør gjøre, og vi har fulgt opp noe av det, men ikke alt, fordi ting tar tid.

11. Har dere noen handlingplaner i tilfelle f.eks. skytjenesten deres går ned?

    – Nei, da er det opp til tredjeparts leverandøren av skytjenesten til å redde oss. Hvis den dagen kommer, da er det slutt for oss.

12. Har du noen tanker om positive eller negative sider med risikovurderinger?

    – Positivt er jo selvfølgelig at du vet noe om hva du driver med da. En ting er at alle vil at vi skal gjøre det. Men det er ingen som prioriterer det høyt nok til at en bruker masse tid på det da. Det er noe vi vil fokusere på fremover, men nå er det å få produktene våre til å virke og ut.

C.6 Interview 6

1. Hva jobber du med?

    – Jeg jobber en del med backend. Jeg er litt mange roller ofte, men blant annet jobber jeg som teamleader, utvikler, og security champion. Ja, og arkitekt. Er vel de rollene jeg har nå. Jeg har vært hos bedriften i flere år.

2. Hvor store team pleier dere å være på prosjektene deres?

    – Det er litt opp og ned, men vi pleier å holde det under 7, fordi vi kjører agile team. Så det blir opp mot 7, helst ikke flere, men vi har hatt opp mot 9 også. Minste team er vel på rundt tre - fire tenker jeg.

3. Har dere noen som jobber direkte mot sikkerhet i utvikling?

    – Ja, det er en del av utviklerne/teamet som har en utvidet rolle som security champion. Deriblant har jeg en slik rolle, det betyr i utgangspunktet at vi har et ekstra fokus på sikkerhet, vi har utdannelse innenfor sikkerhet, og så videre.

4. De som ikke er security champions, får de kursing innenfor sikkerhet de også?

   - De har også en del kursing innenfor sikkerhet, det er jo litt av oppgaven som security champion å videreformidle litt av kunnskapen som vi har. Så vi har jo en del små foredrag med dem og slike ting. Og internt i bedriften, så er det en del interne kurs som alle må gjennom. Det kjøres også ganske bredt i bedriften, som går til alle, nano læring som de kaller det. Hvor vi sender rundt på mailer som de må gå gjennom, ja vi har hatt om kryptografi og passe på at vi ikke legger igjen nøkkelen og alt slik. Alle må gjennomgå disse, de er mandatory. Det blir sjekket om du har gjort det, hvis du ikke har gjort det så får du en hyggelig påminnelse om å gjøre de. Innen for utvikling så er det en del internt som de må ta i tillegg. Så vi har en del små foredrag som går inn på konkrete temaer innenfor sikkerhet.

5. Hvordan jobber dere med sikkerhetsaspektene i prosjektene deres?

   - Jeg jobber hovedsakelig innen forvaltning, men jeg vet jo litt om hva som går og gjelder på sikkerhet. Vi har en såkalt secure-SDLC, som går ved siden av SDLCen som prosjektet skal bruke. Der står det hvilke aktiviteter du skal gjennom. Innenfor når du skal gjøre sikkerhetskrav, når du skal gjøre risikoassesments, og så videre. Den er nært knyttet til Microsofts SDL.

6. Så dere har to forskjellige SDLC, dere har ikke integrert de sammen?

   - De er, hva skal vi si, secure-SDLCen bygger på SDLCen ved at der er to forskjellige dokumenter, men den peker på SDLCen sine faser.

7. Hvem tester sikkerheten hos dere? Gjør dere det selv, eller kommer det eksterne å gjør det?

   - Det er litt ja takk begge deler. Vi gjør noe testing selv, testerne våre har jo en viss basis kunnskap om en del sikkerhetaspekter. I tillegg, for å produksjonssette noe stabil funksjonalitet, så må det gjennom en såkalt pen test Dette gjøres av vår sikkerhetsavdeling, eller så får vi også eksterne konsulenter inn som gjør disse testene.

8. Mener du det jobbes nok opp mot sikkerhet, eller føler du det burde jobbes mer med?

   - Jeg tror vi ligger på et nivå som er akseptabelt innenfor det vi holder på med. Og jeg føler det ikke er noe betalingsvillighet for folk rundt, for slike tjenester som vi holder på med skal jo ikke koste noe. Selvfølgelig kunne vi hatt bedre sikkerhet, og gjort enda mer, det er helt sikkert tilfelle. Men, hvis vi skal konkurrere i markedet i forbindelse med å utvikle og klare å levere i den stand som andre gjør så blir det liksom det nivået vi ligger

på. Men vi er nok ikke de værste i klassen tenker jeg, men det burde vi jo ikke være heller. Selvfølgelig kunne vi brukt mye mer tid på sikkerhet.

- Til syvende og sist så blir det jo slik at hvis man skulle gjort det enda bedre, så ville man jo økt kostnadene. Altså, kostnadene på tjenesten, og der. Og da konkurerer vi med firmaer i India og Russland, som sannsynligvis gir blanke fanden i stort sett det meste, og da, ja. Man må legge det på et nivå som er fornuftig tror jeg. Og jeg tror vi ikke er så langt unna, vi kunne sikker gjort mer men.

9. Vet dere hvilke sikkerhetstrusler dere er mest utsatt for?

   - Det er nok veldig prosjekt til prosjekt. Jeg jobber mye med backend tjenester så du kan jo si får vår det så er vi jo mindre sårbare enn veldig mange andre. Det eneste vi har er noen endepunkter ut mot internett, og en del XML filer og slike type ting. XML kan jo forsåvidt inneholde ganske mye rusk. Mens andre avdelinger har jo rene frontend ut mot kunden som har en helt annen vinkling på det. De har heller alle disse typise OWASP top 10 sårbarhetene. Mens ja, det blir litt tjeneste til tjeneste. Når det gjelder hardwaretjenestene våre, så er jo sikkerheten helt sinnsvak. Derfor har vi liksom hele spekteret, og det avhenger fra tjeneste til tjeneste. Hvor jeg jobber, er det flere personvernskonekvenser hvis noen med onde hensikter kommer seg inn.

10. Har dere gjort noen risikovurderinger på forhånd av sikkerhetsutvikling?

    - Nå har jeg for det meste jobbet i prosjekter som allerede er startet, men nå har vi noe som vi kaller et sikkerhetshjul. Det vil si at alle tjenestene vi har blir vert år vurdert på nytt, dette er samme type risikovurdering som prosjektene gjerne må gjøre tidlig i fasene deres. Så sån sett så har jeg jo vært borti det. Da ser man som oftest på hvilke typer trusler vi har, hvem kan benytte seg av tjenestene, det blir typisk "gitt at person hadde kommet på tjenesten...", det blir typisk på dette nivået her. Men alle prosjekter er pålagt å gjøre det, det vet jeg, men jeg har stort sett kommet inn i prosjekter når dem er i gang. Og jeg jobber nå i forvaltning, som vil si mer med videreutvikling av eksisterende produkter, og da blir det ikke helt det samme.

11. Har du noen tanker om positive og negative sider med risikovurdering i utviklingsprosjekter?

    - Den er jo i utgangspunktet utelukkende positiv bortsett fra det økonomiske. For en oppdager jo ofte ting som en må løse, og de tingene må man jo ofte bruke ressurser på. Utover det ser jeg ikke noe negativt med å gjøre en risikovurdering, det gir jo stort sett bare noe.

12. Har dere handlingsplaner for å håndtere eventuelle angrep?

    – Det er jo stort sett risikoavdelingen sitt hovedområde. Vi blir sannsynligvis angrepet ofte, men de har mitigation plans for hvordan dette håndteres. Det er jo en del av hvordan disse risikovurderingene vi gjør årlig skal inneholde, "hva gjør vi hvis de treffer" også vurderinger for sannsynlighet og konsekvens, risikomatrise.

13. Tror du denne risikoanalysene hjelper med sikkerheten?

    – Ja, det gjør den jo. Absolutt. Jeg vil si at når jeg gikk fra å være utvikler til å bli security champion og tok en del kurs fra bl.a. SANS, så var det en del ting jeg ikke hadde tenkt på før. Det setter et helt annet tankesett fra når du er utvikler, ja hva kan jeg si. Før tenkte jeg ikke så mye over hva jeg la i loggen, den kunne jo ikke brukes til noe, det er jo bare jeg som leser den. Men må tar man jo disse metodene inn i andre verktøy og disse verktøyene viser det gjerne via HTML osv. Risikoanalysen og risikovurderingen er jo kanskje med på å endre hvordan man tenker som utvikler. Derfor syns jeg det er viktig å ha mange med på de tingene, ikke fordi de kanskje kommer opp med de viktige risikoene, men når du sitter å koder så kommer du på at oi, jamen, det her kan jo være ett eller annet.

C.7 Interview 7

1. Hva jobber du med?

    – Vi drifter programmer for våre kunder. Det vi gjør er at vi lager de tekniske systemene og drifter tjenestene våre i tillegg, markedsføring og forslag til ting kunden kan gjøre med tjenestene.

2. Da er det dere som håndterer persondataene?

    – Ja, vi er databehandler for alle kundene våre. Så vi har masse persondata i databasen. Derfor er sikkerhet en stor del av det vi jobber med. Vi lagrer mest kontaktinformasjon, men også atferdsdata som hva som er populære features, hvilken interesser brukerne har, sporing på bevegelse ved hjelp av beakons. Vi plasserer ut en del cookies på flere kampanjer, og prøver å kjenne igjen profiler på ulike platformer for å gi tilbud til diverse brukere. Det er veldig store mengder data som ligger i databasen.

    – Min rolle er teknisk prosjektleder, når vi signerer en ny kunde, så havner det typisk på bordet mitt og jeg må ta ansvar for å levere det vi har sagt vi skal gjøre. Det kan være oppsett av systemer vi har fra før, og til utvikling av apps til kundene og levere det.

3. Hvor mange er det i teamet du jobber med?

   – Det er veldig forskjellig for hvilket type prosjekt det er. Men ofte er det to utviklere kanskje, 1 tester, 1 designer, og en markedssimulator. Så, ja, 5 stykker. Vi har ingen som jobber med sikkerhet.

4. Har utviklerne deres hatt sikkerhetsutdanning?

   – Det tror jeg er ganske varierende. De som sitter på app delen har sannsynligvis ikke hatt det, det er mange unge folk, interns som jobber med det. Så da er det rett fra skolebenken. De har jo sikkerhetsfag som en del av selve opplæringen, det har de. Gjennom utdanningen tenker jeg på da. Vi har også noen mer erfarne folk som sitter på backend, men vi har ikke noen formell opplærings løp eller krav eller noe slikt.

5. Hva jobber dere med innenfor sikkerhet i prosjektene dere har?

   – Det jeg kjenner til i alle fall så er det sikring av data som går i kommunikasjon mellom app og backend, at det er kryptert og går over en sikker protokoll. Vi bruker skytjenester for lagring av data. Der forventer jeg at det er satt opp på en sikker måte. Det er det forholdet jeg har til de tekniske løsningene våre.

6. Så det blir veldig opp til å stole på de som leverer tjenestene dere bruker?

   – I mitt perspektiv så er det det. Men utviklerne har jo et annet forhold til det. For det prosjektet jeg brukte som bakgrunn til spørreundersøkelsen, har et annet forhold til sikkerhet. Alt fra app til backenden og hele porteføljen da. Da vi startet dette prosjektet var det interne sikkerhetsfolk fra kunden som var inne i prosjektet, i tillegg til at de hadde leid inn to eksterne firmaer med fokus på sikkerhet og testing av sikkerhet.

7. Var det da disse eksterne firmaene som drev med testingen?

   – Ja, de fikk appen, og testet fra ende til ende.

8. Testet dere selv også?

   – Det kan jeg ikke si helt med sikkerhet, men vi hadde fått en rekke med krav både fra kunden og de eksterne firmaene. Derfor vil jeg anta at dette ble testet hos oss før vi sendte det videre.

9. Har dere satt opp et trusselbilde på hva som er farlig for deres produkter?

   – Nei, ikke som jeg kjenner til. Det er i alle fall ikke noen fast prosess på det. Om det gjøres av utviklerne på deres avdeling er jeg litt usikker på. Men om jeg skal gjette så tipper jeg nei.

10. Vet du om dette ble gjort i prosjektet du brukte som bakgrunn til undersøkelsen?

    – Det er jeg også litt usikker på, jeg vil jo gjette at de eksterne firmaene satte opp det. Og testet ut fra det. Men vi har ikke noe dokumentasjon på prosjektområdene som vi hadde fått tilsendt i alle fall.

11. Gjør dere noen risikoanalyser på prosjektene deres?

    – Vi gjør vanlige prosjekt risiko analyser, det gjør vi jo. Men ikke noe opp mot sikkerhet til vanlig nei.

    – Nå skal vi gjøre om litt i forhold til ny EU lovgivning, så nå kommer det en del strengere krav med tanke på å dokumentere risikovurderinger. I løpet av høsten vil vi sette opp rammeverk for dette. Det vil derfor bli mye fokus på det fremover.

12. Har du jobbet med risiko før?

    – Ja, det har jeg. I min forrige jobb var jeg leid ut til en kunde som hadde et helt annet fokus på sikkerhet. Der hadde de et rigid opplegg når det kom til sikkerhet og de hadde skoleringer for alt som skulle inn i løsningen. Helt ned til enkle koderammeverk som var nødvendige å vurdere.

13. Ser du positive sider med å gjøre risikovurderinger?

    – Ja, absolutt. For det første så fikk vi luket bort den del småting som hadde sårbarheter. Og ting som ble akseptert til å brukes måtte begrunnes, noe som er greit å ha i bakhånt hvis noe skal oppstå. Det var mange positive effekter med det. I dette prosjektet var tilliten til brukerne ekstremt viktig, derfor spilte det nesten ingen rolle hvor mye sikkerheten ville komme til å koste.

14. Har denne grundige risikovurderingen vært med på å endre tankegangen som utvikler?

    – Det har ikke påvirket meg på noen måte at jeg har gjort noe med det nei. Men jeg kjenner jo til det hvis det skal være noe behov for det, men jeg har ikke vært en fanebærer for risikovurderinger. Det har ikke vær en prioritering for oss nå som vi er på litt startup nivå foreløbig. Vi har flere viktigere ting vi må ferdigstille først. Sikkerhet går da litt i glemmeboken, og det vil sikkert straffe seg i det lange løp.

15. Frem i tid, tror du at dere vil gjøre risikovurderinger før utviklingen starter?

    – På grunn av det nye regelverket, så blir det jo et krav, og da må vi gjøre det. Hadde det ikke vært et krav tror jeg ikke det hadde blitt gjort. Det blir fort en stor papirmølle.

C.8 Interview 8

In this interview there where 4 interviewees, called person 1 (P1), person 2 (P2), person 3 (P3), and person 4 (P4) in order to separate who is answering.

1. Kan dere si noe om hva dere jobber med?
   - **P1** Jeg har akkurat begynt i sikkerhet. Jeg har vært trainee i bedriften, og har da vært hospitert i sikkerhet og vært med på noen risikovurderinger der. Jeg er utdannet forvaltningsinformatiker, med hovedfokus på informasjonssikkerhet. Og risiko er en del av det jeg kommer til å jobbe med fremover.
   - **P2** Jeg jobber også da i sikkerhet. Jeg jobber ikke noe spisset ned mot noe konkret, jeg har teknisk bakgrunn og har både system og infrastruktur oversikt. Jobber litt med dette og styringssystemer, sette krav, styringer og premisser. Ja, jeg jobber ganske bredt.
2. Kan dere fortelle litt om prosjektene deres?
   - **P3** Jeg jobber med modernisering. Det er et prosjekt som går over 4 år. Dette er ett av flere prosjekter som går på fornying av prosesser. Vi flytter løsningene over på en nyere platform, og jobber med bl.a. infrastruktur, og styringer innenfor sikkerhet.
3. Hvor mange jobber med sikkerhetsprosjekter?
   - **P4** Det er alle av oss. Alle vi jobber med sikkerhetsprosjekter, vi har egentlig to roller; vi er egentlig rådgivere i prosjektet, så vi jobber både med sikkerhets arkitektur og risikoanalyser. I den grad vi har resurser til det.
4. Jobber utviklere også med sikkerhet hos dere?
   - **P3** Hvis du tar prosjektet vårt, så er det slik at vi har en av arkitektene som er sikkerhetsansvarlig, som da ivaretar bl.a. informasjonssikkerheten i løsningen, som sørger for at det skrives krav til løsningen. Så er det utviklerne som utvikler i henhold til de kravene. Og i det arbeidet med å beskrive kravene så lærer jo den personene litt opp, og det som finnes av standarder og slik kommer fra ..
   - **P4** Vi har et styringssystem i sms, sant, hvor mange av kravene ligger.
   - **P2** Så brukes jo da risikostyring, testing, og revisjon, som et virkemiddel for å se at produktet holder vann. I tillegg til gjenbruk av vedsatte og godkjente kommunikasjonsstandarder og gjenbruk av noen felleskomponenter som er med på å løse en del grunn funksjonalitet, som du må kunne

forvente. Som autentisering, autorisasjon, tilgangskontroll som da gjør at utviklerne ikke trenger å finne opp den type ting på nytt og på nytt og på nytt. At det er velprøvde ting og det er sertifisert og vi har da kontroll på det fra begynnelsen av. Så når du da starter med å lage noe foretningsfunksjonalitet så starter du ikke med blanke ark, men du har en del rundt deg som hjelper deg med å få på plass den sikkerheten som du skal ha rundt.

- **P3** Og når det gjelder selve risikovurderingene, så gjorde jo vi en risikovurdering for vårt prosjekt med da støtte fra itsikkerhet. Og da var vi i utgangspunktet vel 5 personer som var med, da var det noen som var sikkerhetsansvarlige, løsningsansvarlig, produkteiers person og da noen fra itsikkerhet som sammen da kjørte risikovurderingen. Vi var veldig avhengig av metode, og maler, og rådgivning og støtte fra sikkerhetsavdelingen.

5. Hvilke metoder er det dere bruker? Er det integrert i SDL?

   - **P4** Det er integrert i den forstand at man deffinerer hva man skal gjøre disse tingene. Det er ikke noe teknisk større for dette.

6. Det er mer noe dere gjør på forhånd?

   - **P4** Ja, vi har kontaktet prosjektet, det står at de skal ha en sikkerhetsansvarlig og vi er med på å bestemme om vi må ta en fullstendig risikoanalyse eller om vi kan gjøre en litt mer kortsluttet versjon.
   - **P2** Så fins det altså et malverk, og noen dokumenter som er med på å beskrive, og gir deg noe materiale for å vekte da sannsynlighet og konsekvens og slike ting. Slik at det blir litt konsisens i metodikken i det produktet du lager.
   - **P4** Det er ikke noe spesiell fra oss, det er bare generelle ting hvor vi ser på sannsynlighet og konsekvenser. Prinsippene er jo helt vanlig men de verdiene som man bruker for konsekvensene, eller hvordan man kommer frem til sannsynligheten, kanskje vår egen.
   - **P2** Så har man jo predefinerte eller noen standard betraktninger rundt hva som da er konsekvenser da. Litt slik som økonomi, liv og helse, omdømme. Vi har liksom i utgangspunktet noen slike ting som er viktig for bedriften da, som du kan ta utgangspunkt i når du skal begynne dette tankearbeidet med analysen.

7. Har dere en liste med relevante trusler?

   - **P4** Vi har en liste over trusler, så har vi begynt med å samle en hendelsesliste, en slik typisk hendelsesliste. Det er i progress.

8. Da samler dere inn for hele selskapet, og ikke for prosjekt til prosjekt?

- **P4** Ja, deg gjør vi. Så det er veldig mye gjentakende.
- **P3** Var det ikke den listen med mulige trusler som ble hentet fra en samarbeidsorganisasjon som bedriften var en del av.
- **P4** Ja, det er våre egne erfaringer, pluss en del andre. Så vi prøver å systematisere dette mer enn det vi gjør i dag.

9. Før dere digitaliserer løsningene deres, setter dere opp hvor mulige sikkerhetshull kan oppstå?
   - **P4** Ja, det første skrittet i en risikovurdering er å definere det objektet som man skal risikovurdere. Og da ser man selvrådighet og omgivelsene. Basert på den så kan man finne ut hvor det kan oppstå problemer.
10. Så dere bruker denne listen videre når dere skal lage løsningen?
    - **P4** Ja.
11. Får utviklerne uten en bakgrunn i sikkerhet noen kurs om det?
    - **P2** Vi tilbyr i alle fall kurs på, kall det websårbarheter og andre sårbarheter i tjenester du lager som går over HTTP. Det er et konkret tiltak for utviklere og innleide konsulenter.
    - **P4** Typisk OWASP top 10, som de burde vite, men de skjønner disse da.
    - **P1** I tillegg så er det sikkerhet sin oppgave å drive informasjonsarbeid omkring sikkerhet, og bl.a har vi hengt oss på dette med nasjonal sikkerhetsmåned i oktober. Også har vi en del andre løpende tiltak. Bl.a kommer det Nano læring. Det er vel junglemap som har det, som nå har kjørt det. Da kommer det noen sånne små drypp igjennom hele året, for å få en slik reminder hos folk. Det tror jeg er veldig viktig. Da har man, kan ha større presentasjoner for alle ansatte, og ikke bare utviklere, men også for de andre i bedriften.
    - **P4** Men, det er altså en utfordring, de som kommer inn som utviklere er kanskje ikke helt så gode på sikkerhetssiden som vi skulle ha ønsket.
    - **P2** I tillegg til den generelle sikkerheten, så er det jo vårt domene, forstå domenet, forstå risikoen rundt den virksomheten vi driver. Hvilke type data er det vi holder på med, klassifisering av de og hva skal til for å sikre de og hva er godt nok. Det får du ikke gjort på sidelinjen, det må jo bakes inn i prosjektet for å få den forståelsen om hvilke data det er vi sikrer.
    - **P3** Så er det kanskje også muligens slik at vi, også i bedriftens prosjektstillings metodikk har med referanser til bl.a. hva som kan gjennomføres av sikkerhetsvurderinger og sikkerhetsrisiko. Det tror jeg også kanskje er viktig at det er tidlig på prosjektet, eller noe. For det er lett at de glemmer det.

- **P4** Men det er alltid en del funksjonalitet som skal leveres til en gitt dato, og sikkerhet blir fort plagsom, for å si det slik. For å holde tidsfristen.
- **P2** Så det handler jo om kost / nytte. Dette er en formalisert prosess for å definere kost / nytte i mange tilfeller. Du skal hele tiden gjennom prosjekter gjøre valg, noe skal formaliseres og noe trenger ikke så stor grad av formalisme. Det er jo det det er, det er et verktøy for å ta valg bassert på noen standard input.
- **P2** Det er aldri noe veldig klart ja/nei svar på det, det er ofte litt strikk i det hele her. Du kan være super paranoid og ikke ta risk, og du kan være veldig der ute og ta risk. Du må liksom finne hvor skal vi være på denne scalaen her da. Så det er mye sunn fornuft bakt inn her. Igjen se på hva slags virksomhet er vi.
- **P1** Det finnes ulike måter å ta risk også. Man har jo f.eks firmaer som tar business risk, hvis man velger å kjøre alt man eier og har over i skyen, og så krasjer skyen, så er man jo konkurs, da er det jo ikke noe mer. Men det betyr jo ikke at man er noe risikovillig i forhold til akkurat slike ting.

12. Har dere merket forskjell på å jobbe som konsulenter og å jobbe med prosjekter for egen bedrift?

    - **P4** Ja, det er veldig lett å jobbe som konsulent. Man kommer inn og vet at noe er galt, så leverer vi en rapport. Nå jobber vi for organisasjonen, og det er der den utfordringen ligger, som en konsulent ofte gjerne ikke har. Det er alltid en tung prosess å få ting inn i en organisasjon.
    - **P3** Det er også litt, jeg har fått inntrykk av fra der jeg jobbet før, og jeg kjenner igjen veldig mye av den samme metodikken for å kjøre risikovurderinger og få på plass de tingen og slik. Den var veldig lik, men jeg tror kanskje at man har litt større deler av løsningen her er utsatt for større risiko. I alle fall siden vi håndterer fortrolig informasjon, og en god del sensitiv informasjon. Derfor setter vi jo et stort fokus på det, og kompetansen her er jo mye høyere. Men tilnærmingen og særlig den risikovurderingsmetodikken er veldig gjenkjennbar.
    - **P4** Det er ikke kun it vi jobber med. Vi jobber også med prosesser og fysisk sikring til datarom, og bygninger og slik. Det betyr at det er mer enn bare it.

13. Føler dere at dere er rustet til å håndtere angrep som kommer?

    - **P4** Det er veldig synlig om noe skjer. Så, ja vi er ganske utsatt for omdømmetap.
    - **P1** Mitt inntrykk er at det er blitt jobbet med, når jeg har vært på kurs med andre så er mitt inntrykk at vi her i bedriften er kommet langt, både

når det gjelder etableringen av isms, og måten vi følger det opp på. Jeg skal ikke sitte her å si at vi er kjempe godt forberedt, men vi har gjort, vi har iverksatt veldig mange gode anbefalte tiltak, og ligger sånn sett godt ann da, i forhold til hva vi forventer at vi skal få til.

- **P4** En av de utfordringene for oss er at vi nå blir mye mer åpne til omverden. Og dette øker risikoen vår. Med tanke på elektronisk kommunikasjon.
- **P2** Den tradisjonelle perimetersikringen, utenfor, innenfor, det står litt for fall, du må se på sikkerhet i dybden. At du har sikret tjenestene og at du har synlighet, det er kanskje et stikkord. I tillegg til de preventive tiltakene. Og det er jo også basert på noen vurderinger. Risikovurderinger på hva skjer nå hvis vi begynner å bruke selvbetjeningsløsninger.

14. Når dere tester, leier dere inn eksterne, eller tester dere bare selv?

    - **P4** Begge deler, men vi har ofte folk inne som er profesjonelle på det. Etter at noen har vært inne så lager vi en tiltaksliste som vi følger opp.

15. Har dere satt opp handlingplaner hvis det skjer sikkerhetsbrudd?

    - **P2** Ja, vi har en standard hendelses håndtering som er ganske operativ da, et slags mandat for å operative og så har vi også ganske stort planverk også for avvikshåndtering, og hendelseshåndtering, ned på strateginivå. Dette legger opp til de store krisene, og katastrofeplanlegging. Så du har helt fra håndtere virus og kryptografi opp til de store problemene. Så vi har planlagt å kjøre øvelser, og det jobbes med det her.

16. Har dere noen tanker om risikovurderinger? Positive og negative sider.

    - **P4** Det er veldig nyttig, men det kan være ganske ressurskrevende. Vi har ikke kapasitet til å gjøre alle prosjekter, vi må prioritere. Så det er egentlig ressurser som er den største hindringen.

17. Ser dere nytteverdien i å gjøre risikovurderinger?

    - **P4** Ja.
    - **P3** Jeg tror det er viktig også, sett fra prosjektets side at vi, hvis det nå er slik at den siste risikovurderingen vi gjorde viser seg å være mangelfull, vil vi jo jobbe videre til vi vet hvordan det skal gjørdes, men det gjør jo også slik at vi må justere oss inn i utviklingen. Så sånn sett gir jo risikovurderinger en bevisthet slik at vi får vist frem en del gjennom den siste vurderingen vi gjorde, slik at vi kan gjøre flere tiltak videre for løsningen. Som hvis vi f.eks. ikke hadde gjort det så, og bare skulle stole på konsulentenes og utviklenes og arkitektenes godtbefinnende for sikkerhet i løsningen, så er ikke det godt nok. Vi må detfor ha en bevist

prosess rundt dette og sette oss ned å vurdere hver av det og hva gjør vi med det. Hvilke tiltak er nødvendige og hvilke er, for man er jo ikke 100% sikker på at. Det er jo det store temaet.

- **P4** Men verdien i det er jo det samme som for utvikling, jo tidligere vi finner feil jo billigere er det å fikse.

18. Dere har veldig lange prosjekter, tar dere risikovurderinger på ny underveis?

    - **P4** Ja, særlig hvis det er vesentlige endringer. Så må du forandre risikoanalysen, og den skal stort sett tas med i prosjektet.
    - **P3** Det er sånn sett et krav om at vi skal ha vært gjennom risikovurderingen før man produksjonssetter løsningen. Det regner jeg med at de fleste av oss gjør faktisk. For vårt prosjekt har vi ikke planlagt alt før vi begynner med utviklingen så noe vil jo jobbes med fortsettende og da vil det vi skal produksjonssette være tema for neste risikovurdering. Pluss at vi har en løpende dialog med flere prosjekter om arkitekturen. Slik at det ikke er slik at vi kommer inn, gjør en risk analyse og så forsvinner igjen. Men vi har en løpende dialog og bl.a. på arkitektur siden.
    - **P2** Og da er det jo gjenbruk. Gjenbruk av metoder,gjenbruk av teknologi og gjenbruk av prosesser som da gir deg en slags grunnsikring her.
    - **P3** Det som er litt viktig fra en prosjektleders ståsted vil jo da være at vi gjør en estimering om hvor mye vil dette faktisk ta. Skal man tidlegge det. Med tanke på sikkerhet så må vi jo vite med bemanning og hvor mye dette kommer til å koste. I prosjektene blir sikkerhet fort bare en kostnad, du får ikke noe ut av det, du vil ikke få noen kravpoeng fra det.