TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Jaana Metsamaa IVCM178196

FRAMEWORK FOR MEASURING AND MAXIMIZING SECURITY FEATURE IMPACT IN BUSINESS TO BUSINESS SAAS PRODUCTS

Master's thesis

Supervisor: Andro Kull
PhD

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Jaana Metsamaa IVCM178196

RAAMISTIK TURVAFUNKTSIOONIDE MÕJU MÕÕTMISEKS JA MAKSIMALISEERIMISEKS *SAAS* RAKENDUSTES

Magistritöö

Juhendaja: Andro Kull
PhD

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Jaana Metsamaa

12.05.2019

Abstract

In this thesis, the author developed and tested a framework for business-to-business (B2B) Software as a Service (SaaS) companies to measure and maximise the impact of implementing customer-facing security features. The framework was tested with B2B SaaS software due to ease of access to a test group. The author believes that the framework can be used without the need of major adjustments in business-to-consumer (B2C) software and other types of software like desktop applications or proprietary hosted in the cloud software not only not only SaaS.

The thesis consists of three parts: first use of the perception of security is proposed as the novel metric to quantify the impact. Next, the Net Promoter Score (NPS) framework is adapted to provide the process of measurement of the perception among customers. Finally, the KISCAP model of factors that impact the perception of security among users is adopted to software product development process to find and prioritise the greatest opportunities for improvement. It is important to note that the thesis does not intend to promote deceiving users to perceive software more secure than it is. The thesis proposes a framework that can be used to quantify the impact that has gone into making software more secure and support getting the stakeholder buy-in for continuous investment into making software more secure.

Finally, that developed framework was tested with customers of a B2B SaaS application, analysis of the results and feedback from the stakeholders was collected and analysed for further improvements.

This thesis is written in English and 55 pages long, including four chapters, 19 figures and 7 tables.

Annotatsioon

RAAMISTIK TURVAFUNKTSIOONIDE MÕJU MÕÕTMISEKS JA MAKSIMISEERIMISEKS SAAS RAKENDUSTES

Selles magistritöös töötati välja ning testiti raamistiku B2B SaaS ettevõtetele, et mõõta ning maksimaliseerida turvafunktsionaalsuse arendamise investeeringute mõju.

Töö koosneb kolmest osast. Esmalt valitakse analüüsi tulemusena klientide tunnetuslik turvalisus rakenduse kasutamisel, kvantitatiivseks meetrikaks turvafunktsionaalsuse arendamise mõju mõõtmiseks. Järgnevalt kohandatakse selle mõõtmiseks kliendi soovitusindeksi raamistik (inglise keeles: Net Promoter Score). Seejärel kohandatakse TMTKTV raamistikku (teadmised, mõju, tõsisus, kontrollitavus, teadlikus ning võimalikkus aspektidest mis mõjutavad kasutajate tunnetuslikku turvalisust tootearendusprotsessi, leidmaks ning prioritiseerimaks suurimaid võimalusi antud toote kasutajate tunnetusliku turvalisuse suurendamiseks.

Viimaks katsetatakse seda väljatöötatud raamistikku ühes firmadevahelises tarkvarateenuses kasutajate tunnetusliku turvalisuse skoori leidmiseks ning järgnevate plaanide prioritiseerimiseks. Katsetulemusi ning ettevõtte sidusrühma tagasiside analüüsi põhjal teostatakse analüüs ning pakutakse välja tulevased võimalikud uurimisteemad ja raamistiku parendusettepanekud.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 55 leheküljel, 4 peatükki, 19 joonist, 7 tabelit.

List of abbreviations and terms

ALE	Annual Loss Expectancy
API	Application Programming Interface
B2B	Business-to-business
B2C	Business-to-consumer
CIA	Confidentiality, Integrity, Availability
CRM	Customer Relationship Management
KISCAP	Knowledge, Impact, Severity, Controllability, Awareness and Possibility
KPI	Key Performance Indicator
mALE	Modified ALE
NDA	Non-Disclosure Agreement
North Star metric	Most important metric for a team, improving which is their main goal
NPS	Net Promoter Score
Perception of security score	10-point rating given by the user to the question "*How secure do you feel about your business data in service X?"*
RFP	Request for Proposal
ROI	Return on Investment
ROSI	Return on Security Investment
ROSSI	Return on SaaS Security Investment
SaaS	Software as a Service
SME	Small and Medium Enterprise

Table of contents

List of figures

List of tables

1 Introduction

The need for companies to invest in information security is made evident almost every day with news of security incidents, vulnerabilities and data breaches in connected systems everywhere. It used to be that the primary issue for companies in migrating to cloud providers when required services were available was cost. Today it is vice versa; it is often more cost-effective for an Small and Medium Enterprises (SME) to adopt a Software as a Service (SaaS) application in the cloud for common business objectives like e-mail, project management, customer relationship management and similar than build and then maintain such software in-house. The cost of cloud solutions is no longer the main concern. That said, the cost is also not the only concern to be considered, for very specialized businesses there may not even exist a cloud alternative to on premise self-developed software. In cases where the SaaS solution is an option, companies today see cloud data security as the primary risk they are facing [1]. That is an overall risk, not only a risk in the IT area.

SaaS applications require little to none in-house IT maintenance and usually come with constant upgrades and can scale as the business grows. Ease of management, however, comes with a price - most SaaS applications are like a black box. Customers often have no visibility into what data is accessed by whom, where and for what purpose.

Potential data access by third parties, however, is not the only risk. In an analysis from 2018, Gartner predicts that “up to 95 per cent of all data leaks in the cloud through 2020 will be due to an incorrect configuration, account management or mistakes by IT departments, rather than the vulnerability of the cloud provider” [1]. Therefore, there is a need for security features in SaaS applications that are both robust and easy to use to mitigate different types of threats to data security even without in-depth specialised training.

There has not been much research into how much available security measures impact a company’s decision on which SaaS provider to buy. Related research has been done 8 years ago in identifying factors affecting perception in business-to-consumer software

products of information security and their impacts on IT adoption and security [2]. Qualitative research amongst B2B SaaS customers of a customer relationship management (CRM) product, however, concluded that the level of security features is not a driving force in choosing such type of a cloud software provider. Security can be a reason why not to choose a specific one [3]. That said, the importance of security in selecting software will depend on the type of the customer and software needed. For example when choosing a centralized password management application for the whole company security would be the primary aspect to consider as opposed to choosing a voice over IP (VoIP) provider, call quality would come first and then other aspects would be considered (and prioritising call quality would always be more important as before fixing that no-one would even start assessing its security).

The concept of calculating return on investment (ROI) applies to implementing security features like to any other investment. Yet, as security measures are not always the driving force in product selection, then this means that any new customer acquired and revenues from them cannot be attributed to those security measures, and the impact of these developments (ROI) cannot be measured.

In product development where the product is used by multiple customers, features that are requested the most and/or get highest user engagement are ranked with top priority for development as these are believed to yield in highest returns. Such feature requests are most often (but not only) communicated in conversations with the day to day users of the applications. Unfortunately, information security and related features are not expected to have high regular user engagement and mostly do not break the noise barrier and do not stand out in such lists.

Product development is not limited to customer requests only. Companies often also develop features and products that have not been directly requested by any customer, but have great potential to solve a customer pain and bring in a positive return on investment.

There is a widely used and thought formula for calculating Return on Security Investment (ROSI) for internal information security programs and securing infrastructure.

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

Return on security investment (ROSI) is calculated by accounting for the monetary loss reduction gained and cost of it as mostly investment into security is seen as loss reducing not profit bringing investments [4]. Although potential losses from incidents and their reductions through mitigations are often overestimated, these are still valuable indicators that can inform decision making.

There is no framework (or a one that is widely known) for understanding the return of SaaS Security investment (ROSSI) which would help answer the questions:

- How to define and quantify the impact of security features developed into a SaaS application?
- Could such quantifiable measure serve as the most important metric for the team that is responsible for developing customer facing security features?
- Have enough security measures been implemented or should investment into the area continue if not even be increased?

In this thesis, the author aims to develop and test a framework for B2B SaaS companies to measure and maximise the impact of implementing customer-facing security features.

This paper focuses on customer facing security measures. Examples of such features are multi-factor authentication, user roles, data visibility, permissions, password strength requirements and similar. Application and network level security features like database encryption, backups, network security and similar are not considered as customer facing security features in the context of this thesis. This paper also restricts the scope to SaaS applications where the multiple subscribers can license the use of software that is hosted centrally “in the cloud”. The cost of the license is very often tied to the number of users accessing the software and a variety of features on the selected package. In this thesis other cloud service models where cost can be tied to other aspects like computing resources are not considered. Examples of such models are Infrastructure as a Service (like Amazon Web Services, Google Compute Engine), Platform as a Service (Google App Engine, OpenShift, Windows Azure) or Desktop as a Service (Cloud Desktop Online).

2 Measuring the ROI of SaaS security feature development

SaaS is a licencing model where the subscriber licenses the use of software that is hosted centrally “in the cloud” . The cost of such license is very often tied to the number of users accessing the software and a variety of features on the selected package. The software can often be accessed from anywhere through a web browser or through a thin client.

Specially for more generic SaaS applications, the price of the service is relatively low for a single user. Business models of such services is built on quantity of the customers. According to a top SaaS application review site Q2 Crowd (based on Alexa Traffic Rank [5] [6]), 8 out of 10 top rated B2B SaaS applications [5] were using a variation of per user pricing model. Competition between such SaaS providers is therefore harsh. Addition to product plan prices, customers are constantly comparing features available on different services and are not reluctant to switch providers. SaaS companies are constantly tracking the reasons why a certain customer left or what were the features that the prospect found missing that made them not convert to a paying customer. These reasons are a constant input to the product development roadmaps that get prioritised based on the impact feature can have to the product usage.

In this chapter, the author explores and compares a few ways of measuring the impact of developing security features to SaaS products. One of the ways is then selected and adapted into a framework for measuring and maximising that impact.

2.1 Comparison of measurement methods for SaaS Security Feature Impact

In this chapter, the author explores and compares a few ways of defining and measuring the impact of developing security features to SaaS products that ideally would be applicable to both potential new and already existing customers and would be as effortless as possible to measure.

- **Calculating ROI**

The easiest and most common way to prioritise product feature development is to calculate the impact on revenues (e.g. new customers acquired) or increase in product engagement. Security features (e.g. access rights, multi-factor authentications etc.) in their nature are not the main things which need to be engaged with often, then engagement as a metric really is not applicable. In order to estimate the impact on revenue of customer facing security features one or two of the following need to be calculated: number of new customers who claim a security feature was the main reason for them signing up or number of potential customers claiming that the lack of (or a low quality of) a particular security feature was the reason for them not to sign up.

- **Calculating Return on Security Investment (ROSI)**

A widely used and taught way of measuring ROSI (Return on Security Investment) is to look at it not as a profit increasing but loss decreasing investment. When calculating ROSI, the total annual monetary loss of an incident is estimated (*ALE* - annual loss expectancy), then how much this loss can be reduced thanks to a remedy (*mALE* - modified *ALE*) is calculated, and the cost of this loss reduction is deducted from the total and the result is divided by the total cost of the investment to get the profitability percentage [4]. Investments with ROSI well over 100% are worthwhile making.

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ Solution}{Cost\ of\ the\ Solution}$$

$$ROSI = \frac{Monetary\ Loss\ Reduction - Cost\ of\ the\ Solution}{Cost\ of\ the\ Solution}$$

This model has been well adopted in the IT industry and become the *de facto* standard for deciding on the investment into information security. Estimating the potential loss and its reduction after applying a remedy is difficult to do for any single company. Calculating the same for all the customers of a SaaS provider would be infeasible due to the bureaucratic burden of collecting the data which customers might not want to disclose. In addition, such a calculation would be very biased towards larger customers with significant potential losses. This approach would also exclude any potential new customer from the impact calculations.

- **Counting incidents per user**

Another option to estimate the effectiveness of security investments would be to monitor the number of security incidents in the CIA triad (confidentiality, integrity, availability) of customer accounts. To counterbalance the fact that some customer accounts have more users than others and therefore are more likely to have security incidents, the metric can be calculated per user account not per company. This metric unfortunately would only be applicable to existing customers and would be relatively difficult to measure as there needs to be a process of collecting this information from the companies who in turn need to have a mechanism of reporting these.

- **Measuring the perception of security**

The methods considered so far have all had a significant downside of bringing high bureaucratic burden to either the SaaS provider, the customer or both. In addition, due to the confidential nature of the data required in the calculations, they could be only applicable to already existing customers with whom Non-Disclosure Agreements (NDA) would support sharing such information. Knowing that security features are already considered during the SaaS selection progress and can have an impact on the adoption of online services we could opt to measure that perception of security that either the potential new or existing customers have of the product [3] [2]. This approach would, therefore, be applicable to both potential new and existing customers and would require no confidential information to be shared. Compared to other methods mentioned perception of security is a subjective rating and will be influenced by outside factors like mood, previous experiences and similar. The author finds that one needs to be aware of this fact but believes that when measured on a quantitative scale where ratings

from multiple people are combined, it will provide an objective estimate. A summary of this analysis is visible in Table 1.

	Applicable to potential customers	**Applicable to existing customers**	**Bureaucratic burden (low, medium, high)**
ROI	✗	✗	low
Monetary loss reduction (collective ROSI)	✗	✓	high
Incidents per user	✗	✓	medium
Perception of security	✓	✓	low

Table 1 Comparison of different measurement methods discussed in this chapter

In this chapter different ways of measuring the impact of security feature development were compared considering three main dimensions - applicability to potential new customers, applicability to existing customers and the bureaucratic burden it would bring to the SaaS company and its customers. According to the comparison, the only approach that would be applicable to both potential new and existing customers is to measure the perception of security with relatively low bureaucratic burden when measuring. In the following chapters, the author will propose a framework of how to measure the impact of security feature development on the perception of security among potential new and existing customers.

3 Framework for prioritisation using the KISCAP model

Perception is a key component of human behaviour. “It is the mechanism with which a person evaluates inputs from the external environment, which, in turn, determines his/her behavioural response” [5]. “The gap between the perceived security of an information system and its real security level can influence people's decisions and behaviour” [2]. For example, research has shown the perceived strength of nonrepudiation, privacy protection, and data integrity to be important determinants of e-commerce acceptance [6]. The approach of measuring the perception of security can be universal among both potential new and already existing customers as perception is built already before signing up and early during trial evaluation.

Huang *et al*. identified a six-factor structure that can influence people’s perception of information security, and how people perceive different kinds of threats to information security [2]. They proposed further research where the identified six-factor structure KISCAP: knowledge (K), impact (I), severity (S), controllability (C), awareness (A) and possibility (P) could be applied in the development and evaluation of security methods, guidelines for adjusting perceived dangers of IT appliances [10]. In this chapter, the author explores how security methods could be measured against these six factors and these measurements then used for feature development prioritisation in order to increase the perception of security of the given product or service.

The six factors of the KISCAP model were derived by testing the factors with different Internet hazards like malware, spam, computer viruses and others [10]. This research was done from the perspective of the computer user in the B2C environment. In order to use the perception of security as a metric for prioritisation, there needs to be an understanding which of these six factors can be impacted from the perspective of the product and how.

The six KISCAP features are clustering’s of 20 items that have been known to influence the perception of general hazards that were confirmed also to influence the perception of IT security [10]. Detailed list of each of the 20 elements in the six clusters are visible in Table 2 The six factors of security perception together with the factors grouped into each by *Huang et.al.* .Table 2.

3.1 Adapting the KISCAP model to product development

The KISCAP model was developed from the perspective of the computer user. In order to use the perception of security as a metric for prioritisation there needs to be an interpretation of these six factors from the perspective of the product and how each of them could be impacted by actions from the product provider. In the following chapter the author proposes such interpretation.

- **Knowledge** (familiarity, understanding, control of severity)

Previous KISCAP research showed that threats that people thought to know well, they found to be able to detect easily and therefore perceive these threats as least dangerous [10]. In product development, this means that in addition to developing security measures it is also essential to educate users about the threats their business data is facing and how product features and other measures could help to mitigate them.

- **Impact** (duration of impact, the scope of impact, media attention)

Threats perceived as the most dangerous are expected to be potentially severe and long-lasting consequences. Product features can help users to reduce the duration and the scope of the impact by providing flexible data access controls and data leak alerting.

- **Severity** (personal exposure, voluntariness, the severity of consequence)

Threats to information security can have consequences of different severity. Limiting the severity of any potential threat is one of the key things a product can do to make it both perceived and be more secure. Such security measures might include limiting the amount of data one account could export in a period of time, having integration specific Application Programming Interface (API) keys and similar.

- **Controllability** (preventive control, observability, ease of reduction, reversibility, predictability, catastrophic potential)

Items in the controllability group indicate how much people can control the threats, whether the threats can be prevented, observed, reversed and predicted. If and how much the effects can be reduced, and whether their outcomes are scattered in time and space [10]. Most if not all security features can contribute to improving this category. Examples of basic security features in this group are minimum password strength levels,

multi-factor authentication enforcement *etc*. are in this category. More advanced features might be focusing on increasing observability and threat prediction with robust data access monitoring.

- **Possibility** (accident history, possibility)

"People may perceive a relatively high possibility of being exposed to a threat if they have already been exposed to it in the past." [10] This category represents the "baggage" and experiences that the users have come in contact with. From one hand if the experience with a threat was with the same application the perceived security of the application will be lower. That said, the customers who had such an experience before but still remained as a user will be a lot more perceptive to new security measures added. It would be challenging to impact this factor of the perception directly with any single feature development or communication campaign, but the aim still needs to decrease this as much as possible by developing security features that help keep the number of users in this category, as small as possible.

- **Awareness** (immediacy of effect, known to the exposed)

Similarly, to the Knowledge factor, threats with high awareness and knowledge are perceived as less dangerous through the fact that users feel they can easily detect and then control them. Example of a feature that could increase awareness would be to notify users about new devices logging into their account. Receiving such notifications about users' own devices will make them aware that a device that is not their own is a threat, but they now have a way of quickly detecting it.

In order to impact these six factors and the security perception overall, the security measure proposed needs to increase some and decrease others. The desired effect is added to the detailed listings of the six factors derived from work by *Huang et.al.* [10] and presented in the following Table 2 with green (to increase) and red (to decrease) arrows.

Knowledge	**Impact**	**Severity**	**Controllability**	**Possibility**	**Awareness**
to increase ↑	*to decrease* ↓	*to decrease* ↓	*to increase* ↑	*to decrease* ↓	*to increase* ↑
Familiarity	Duration of impact	Personal exposure	Preventive control	Accident history	Immediacy of effect
Understanding	Scope of impacts	Voluntariness	Observability	Possibility	Known to the exposed
Control of Severity	Media attention	Severity of consequence	Ease of reduction		
Newness			Reversibility		
			Predictability		
			Catastrophic potential		

Table 2 The six factors of security perception together with the factors grouped into each by *Huang et.al.* [10]

From the analysis above done through the lens of product management, it is visible that there are factors that can be impacted more through feature development like Impact, Controllability and Severity. However, considering the nature of some of the factors like Knowledge, Possibility and Awareness, these can be less relevant when considering specific security features to be built in order to either increase or decrease them. This, however, should not mean that they can be disregarded. Developing features is not the only way to increase security perception. In addition, SaaS perception can be improved by improving documentation, marketing campaigns and customer communication. Such campaigns could, for example, educate existing users about potential threats to their accounts and familiarising them with existing tools that they could use. Similarly, SaaS could target the perception of potential new customers by establishing themselves as a thought leader about business data security and what companies could do to manage those risks.

Therefore, the author proposes the complete framework of how the perception of security can be developed and how it impacts products growth. Here the term growth is a simplification of various business goals of the company – it might be additional

customers, extension of features and products sold to an existing customer. All these above mentioned will require customers trust and above moderate perception of security to materialize.

The proposed framework is visualised in Figure 1. The framework consists of the six core factors of perception (in orange) that are each impacted by a variety of security features (in purple) and customer communication activities (in pink). The factors of perception (in orange) together make out the perception of security (yellow). This, in turn, impacts the products Net Promoter Score (NPS), that in turn either contributes to the growth or decline of growth (in green).

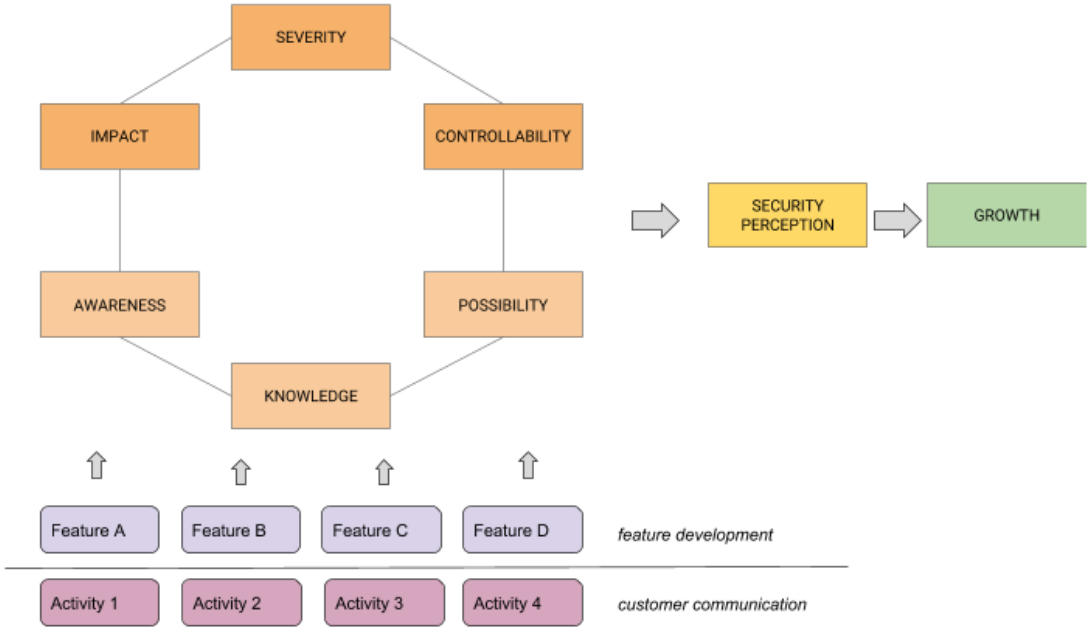

Figure 1 The framework proposed by the author of how the perception of security develops and how it impacts the perception score and growth.

3.2 Developing the customer survey for measuring security perception

In previous chapters, it was concluded that the approach to quantifying security investment impact that would be applicable to both potential new and existing customers is to measure the perception of security with a relatively low bureaucratic burden when measuring. The previous chapter introduced the framework of how the perception of security develops and how it contributes to product growth. This chapter

develops the framework further to support prioritising between potential security investments and later quantify the results.

Baseline perception

In order to improve anything, the current status quo needs to be established as a baseline and possible options prioritised based on their impact:

- First, the perception needs to be quantified to a number that could be observed before and after any features are developed or communication campaigns conducted.

- Second, an understanding needs to be gathered of which of the six factors of perception could be improved the most.

- Third, potential activities need to be rated in terms of their impact on the different factors of security perception.

- Finally, items can be prioritised by the potential improvement to different factors of perception of security.

3.2.1 Net Promoter Score

NPS (Net Promoter Score) is a simple and also very widely used framework for measuring customers feelings towards a company that both companies and customers are used to [8] [9]. As no confidential data is required to share a person's perception, such a survey can be applied to both potential new and already existing customers. In this chapter, the author will explore adapting the NPS framework for measuring the customer's perception of security.

NPS metric was developed by Fred Reichheld, *Bain & Company* and *Satmetrix* which offers a customer experience management platform [9]. NPS is a metric for quickly measuring whether customers are feeling better or worse about the product over time. A significant benefit compared to previous most used customer satisfaction surveys was the simplicity of asking just one question and the speed of which the results could be gathered and also consumed. NPS has become a standard in both digital and non-digital products for measuring customer loyalty and perception. *Google, Facebook, Apple*, *BMW* and *American Airlines* all send out NPS surveys regularly. As NPS surveys are so common among SaaS providers, there are even many purpose-built tools for sending the

surveys out, and many products themselves have NPS style questionnaires built in [8]. This, in fact, can help companies to adopt the framework more easily as existing tools and process are already in place to support it. Figure 2 shows a classic example of an email NPS survey from Apple and on Figure 3 is an example of an NPS survey integrated into an online application JIRA by *Atlassian*.

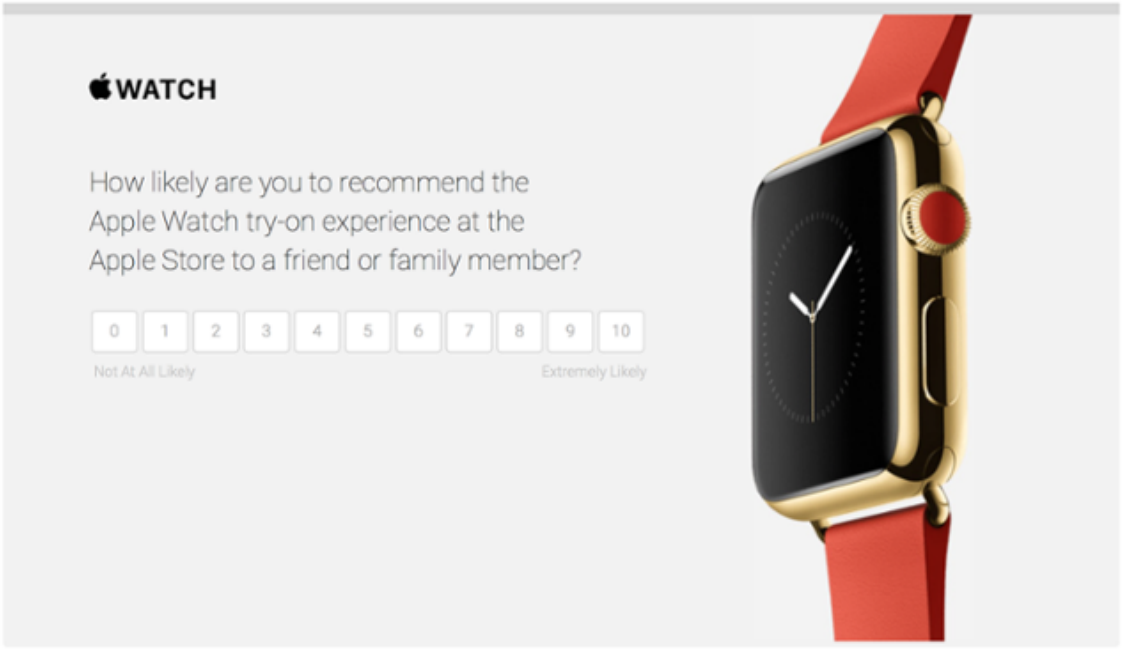

Figure 2 Example NPS survey sent via email by Apple [10].

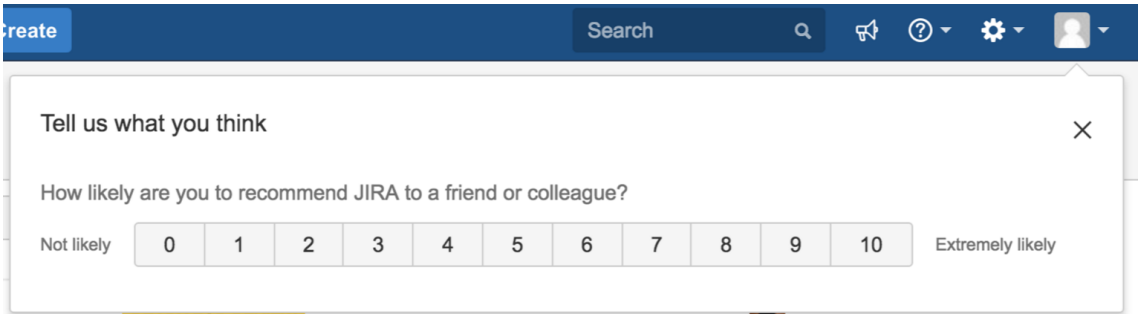

Figure 3 NPS survey integrated into Atlassian JIRA product.

Traditionally NPS survey focuses on a single question: *"On a scale of zero to ten, how likely are you to recommend [company X] to a friend or colleague?"* with an added open-ended question *"What is the primary reason for your score?"* to get further context on the scores and possibly generalise on the results. According to tests conducted by Fred Reichheld, Bain & Company [9].

NPS scores correlated with the growth rate of the company. Therefore, the higher the NPS, the more people actually recommend the service to others, generating growth.

The Net Promoter Score is the percentage of promoters (scores 9 and 10) minus the percentage of detractors (scores 0 to 6). The passive respondents (score 5) are considered not to "move the needle" neither promoting or demoting and are left out from the promoter calculation.

The formula for calculating NPS:

$$NPS = \frac{promoters - detractors}{respondents} \times 100$$

NPS result ranges from −100 (everyone is a detractor) to +100 (everyone is a promoter). Anything over 0 is considered positive. An NPS of +50 is already excellent. Apple has had one of the highest scores in the industry, reaching to 86 in 2016 [11].

3.2.2 Choosing the right question

One of the main reasons why the Net Promoter survey is so widely used and popular is its length - it consists of a single rating with a follow-up question. Web application *SurveyMonkey* is in their own words the largest source of online survey distribution and response collection in the world. Their research done across 100,000 surveys of different lengths showed that adding more questions to a survey will decrease its response rate [15]. In addition, the author knew from personal experience that if the survey was kept short with a rating and a follow-up question, the respondents would be able to respond within the application without needing to open and navigate to a new window, which surely would be an extra step for the user that can cause an additional drop off in the response rate.

Therefore, when developing the survey to measure the perception of security, the goal was to achieve similar results, while keeping the same simplicity of just a single question. It is important to note that this step of finding the right question is not standard for the NPS framework, when surveying for the Net Promoter Score the question is always *"On a scale of zero to ten, how likely are you to recommend [company X] to a friend or colleague?"* with an added open-ended question *"What is the primary reason for your score?"*. The fact that the question is the same for all the NPS surveys, makes

them comparable and avoids bias that could come from *Apple* and *Microsoft*, for example, finding their own single questions to survey. This step is however required in order to develop a similar standard question for perception of security. In this chapter, a few different questions are considered, and the final question selected for the survey.

The final questions considered together with the stakeholders were developed by the author. Unfortunately, there are no other such common questions in the field of product development besides the NPS Survey recommendation question that could have been used. NPS Survey question itself was considered too broad for this context. Most of online material around measuring security on the other hand focuses on internal information security programs and measuring their effectiveness through reduction of risk or number of incidents which is too specific and were disregarded as per analysis in Chapter 2.1.

Final six questions considered together with the stakeholders (product management leadership) and experts in related fields (Data Protection Officer, Head of Customer Research and Product Manager of Security features):

1. How do you rate the security of service X?

2. How do you rate the security of your business data in service X?

The first two questions were disregarded due to the fact that in reality, most customers do not have the skillset to assess the security of the service accurately. In the best case scenario, they could assess specific features not the whole service in general like these questions would require.

3. How in control do you feel over who can see and do what in your service X account?

4. How in control do you feel over the security of your business data in service X?

These two questions focus on two attributes of security perception - control and transparency. As security is not just about knowing and having control, then these questions are not quite suitable.

5. How confident are you with the security of your business data in service X?

From all the previous questions considered, explicitly focusing on security of the data not the broad abstract concept of security only, makes the questions more specific and less vague. The next question focuses on the customers' confidence. Confidence levels in general, about anything, are very individual - some are always more confident than others, and it might not have anything to do with prior experience and knowledge with the topic in discussion. Therefore, it would be very difficult to estimate the implicit bias in these answers.

6. How secure do you feel about your business data in service X?

Next question is focusing on how customers feel about the security of their business data. As the question is only about individual feelings, it does not require special skills. A similar approach of asking about feelings is also used by city governments when measuring citizens' perceptions of security of their neighbourhood [12].

In addition to the question for the rating *"How secure do you feel about your business data in service X?*, NPS surveys often include a follow-up question to allow respondents to give more context to the rating. As asking about feelings about the security is not very common, the additional question *"What's the primary reason for your score?"* is definitely needed to get more context on the ratings and to get an understanding whether the respondents understood the question well.

Conclusion

In this chapter, the author introduced the Net Promoter Score framework and how it is used to measure customer feelings towards a company. The author also explained how using the tools and processes already existing for surveying for NPS will make it so much easier for companies to adopt the perception of security framework as these already exist and they are familiar with them. The author then developed the survey for measuring the perception of security. After weighing different options, the final survey consists of two questions: "How secure do you feel about your business data in service X?" and a follow-up question *"What's the primary reason for your score?"*. This survey can now be easily be conducted by any company using the same tools that they are available (or maybe they are already using) for surveying for the NPS score.

3.3 Prioritising features for security perception improvement

3.3.1 Identifying factors of improvement in security perception

In order to get an understanding where improvements could be made, data needs to be gathered from the customers. Input about security features can be gathered from the same sources as any other product input - customer interviews, research, customer support, sales, social media, reviews and other sources. In addition, security features often get additional attention in RFP (Request for Proposal) documents and vendor checklists often sent to be filled by more established and bigger companies. Next, the feedback collected needs to be mapped as opportunities to improve a specific aspect of security perception as visualised in Figure 4.

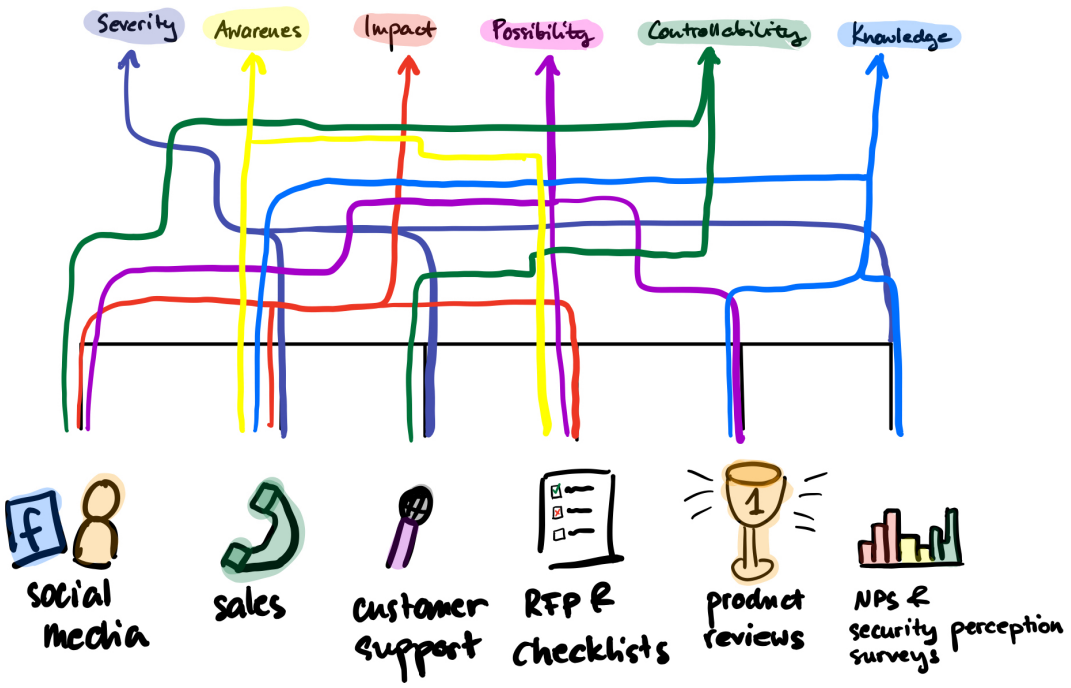

Figure 4 Visualisation of categorisation of feedback into the categories representing the six factors of perception of security. Not all possible paths are visualised. Illustration created by the author.

It is probable that most of the input coming from traditional channels like reviews and customer support cases would end up in the controllability category as customers often focus on asking for specific solutions in such conversations. Less biased picture of where the opportunities are, however, can be achieved by only grouping the comments from the security perception score survey and focusing on which of the aspects needs to be improved in order to improve that specific respondent's score.

The results of the security perception score grouping visualised as a radial graph will help to identify the largest areas of opportunity. This will be the input for the next stage of the prioritisation framework where each activity idea (for maximising the security perception score) is weight against if and how much it impacts each of the six factors of security perception. In a fictional example radial graph created by the author in Figure 5 demonstrates that the Impact factor has the biggest potential to increase the security perception score.

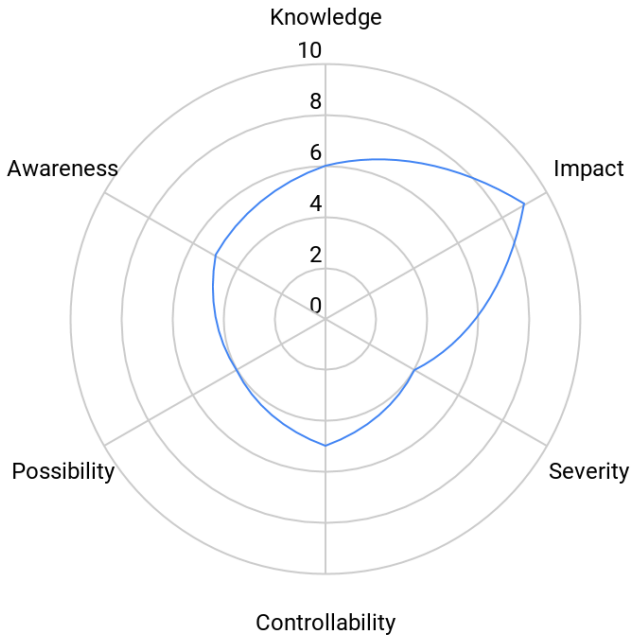

Figure 5 Results of a security perception score feedback visualised as a radial graph with the six factors of security perception.

3.3.2 Evaluating the potential impact on the perception score of each idea

Once it has been identified which of the six perception factors could be improved the most, it needs to be decided which of the improvement ideas can contribute to the improvement with the best cost-benefit ratio.

For this, each idea needs to be rated in all of the categories. Example of how this could be done is in Table 3.

Symbols used in the table:

- ✓ marks a positive impact on the factor in the desired direction
- N/A - the activity has neither a positive nor negative impact on the factor
- ✗ marks a negative impact on the factor

Idea	**Knowledge**	**Impact**	**Severity**	**Controllability**	**Possibility**	**Awareness**
	to increase ↑	*to decrease ↓*	*to decrease ↓*	*to increase ↑*	*to decrease ↓*	*to increase ↑*
Notify users about new devices logged into their accounts	✓	✓	N/A	✓	✓	N/A
Raise minimum password strength requirements	N/A	N/A	N/A	N/A	✓	N/A
A blog post about the benefits of 2FA	✓	N/A	N/A	✓	✓	✓

Table 3 Example evaluation of ideas generated by the author to improve the security perception score.

3.3.3 Prioritising features for security perception improvement

Next, as the potential benefits of each idea are mapped, the cost of implementation needs to be reviewed in order to conduct a Cost-benefits analysis and choose the most profitable course of action that maximises the value against the costs [13]. The cost can be evaluated by using t-shirt-size estimations where each size (S, M, L, XL *etc*.) is an order of magnitude bigger than the previous. The measure could be time, money or something else. For example, S might represent something that could be built in a week or two, M in a month, L a few months and so on [14].

Table 4 is a simplification of Table 3 of improvement ideas where positive impact columns are grouped into the *Benefits* column and all negative impact factors to the *Downsides* column. A new *Cost* column is added to represent a t-shirt cost estimation.

Symbols used in the table:

- Letters K, I, S, C, A, P represent the factor that is impacted either positively or negatively by the idea
- S - the idea can be implemented in a few days
- M - the idea can be implemented in a few weeks
- L - the idea can be implemented in a few months
- XL - the idea can be implemented in a few quarters

Idea	**Benefits**	**Downsides**	**Cost**
Notify users about new devices logged into their accounts	K, I, C, P	N/A	L
Raise minimum password strength requirements	P	N/A	M
A blog post about the benefits of 2FA	K, C, A, P	N/A	S

Table 4 Example of the cost-benefit analysis of the improvement ideas.

It might be tempting to draw conclusions be adding up how many “letters” each idea impacts positively and the relative cost and prioritise the item that has the most benefits with the lowest cost. This, however, should not be done. The letters do represent that there is an impact on the factors of security perception, but there is no quantification of how big the impact is. Similarly, the cost does not take into account which resources would be used for implementation and if they are available. Including such details to

these tables would be quite complicated and would be almost impossible to make it universal. Therefore, additional analysis considering these factors needs to be conducted before making the final decision to either move forward with the implementation or further analysis of a few ideas.

Conclusion

This chapter proposed a new framework of how the six factors identified by Huang *et al*. that can influence people's perception of information security (KISCAP) [2] can be interpreted in product development, used for measuring the impact of user facing security features and prioritising different activities to maximise the perception of security score.

The development of the framework consists of the four major steps:

- First, a process of quantifying the security perception in a 10-point scale through a user survey was introduced so that the score could be observed before and after any potential improvement is implemented

- Second, a process of grouping customer input in a way that it can be understood which of the six factors of perception could be improved the most was introduced

- Third, a process of evaluating potential activities in terms of their potential impact on the different factors of security perception was introduced

- Finally, a process of prioritising the potential improvement to different factors of perception of security was introduced

In the next chapter, the developed framework for measuring the security perception, finding the most significant opportunities for improvement and prioritising potential activities is tested in a SaaS company on real customers and stakeholders.

4 Testing the security perception framework in practice

In this chapter, the author tests the developed framework in a SaaS company with real customers and stakeholders. The chapter gives an overview of how the survey to measure perception was conducted, analyses the results, what conclusions can or cannot be made from them. In addition, the framework, its format, the process of the survey and the prioritisation is analysed, and feedback collected about it from stakeholders. Improvement ideas based on the experience and feedback are also proposed.

Due to confidential nature of the perception of security score of the company where the framework was tested, the actual score will not be shared in this thesis. The author believes that the analysis of the framework can be made nevertheless as the proportion of certain categories of responses and examples of scores given together with the accompanying scores are shared. The author also shares the expectation for the score by the stakeholders and whether the score was higher or lower than this.

4.1 Analysis of the survey results

4.1.1 The target group of the survey

The framework was tested in a customer relationship management (CRM) SaaS company. At the time of the test the company had 85,000 customers, each of whom can have 1 to *n* users. The company offers user based pricing in three different pricing tiers. The survey was sent out to English speaking administrators of the B2B SaaS accounts which had more than five users and who had not received any in-app surveys in the last 30 days. The limitation of at least five users was added due to the fact that research has shown that bigger companies care more about security features and therefore are more "in the target group" of such features whose perception then needs to be measured [3]. The survey was sent as a *Survicate* [15] NPS survey with an in-app *Intercom* [16] chat bubble pop-up within the web app as seen in Figure 6, Figure 7 and Figure 8.

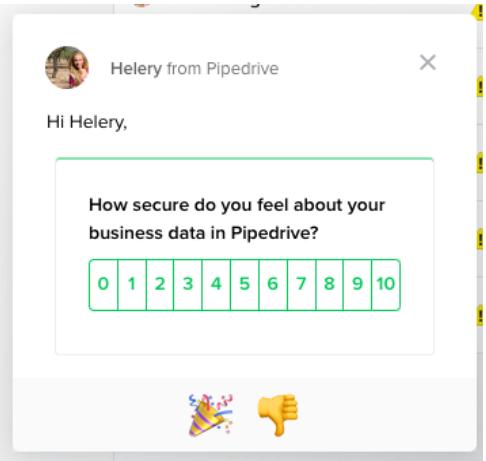

Figure 6 First screen of the security perception score survey shown as a small *"chat bubble"* in the application.

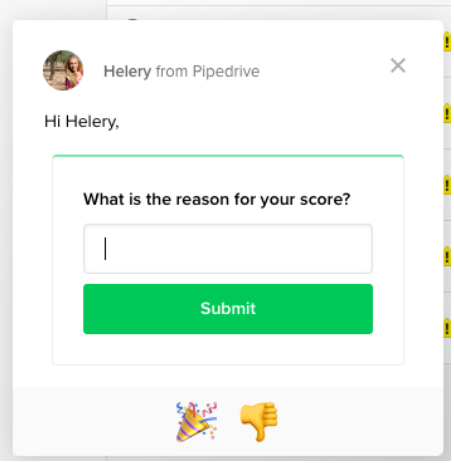

Figure 7 Additional question after the rating of the security perception score survey shown as a small "chat bubble" in the application.

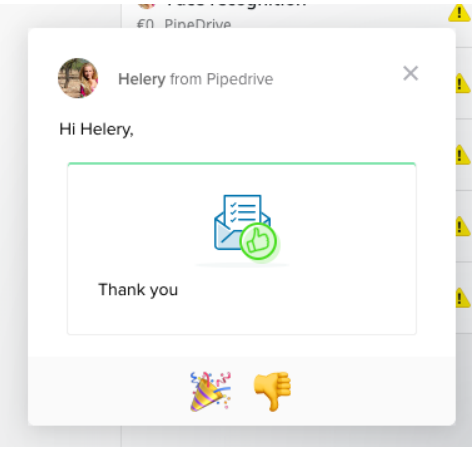

Figure 8 Thank you note after the customer responded to both questions.

The plan was to run the survey until 100 responses were received which considering the average user count of such customers would represent the decisionmakers from a significant number of the users. In total, the survey received 107 responses.

4.1.2 Analysis of the survey responses

One of the uncertainties in sending the survey out was whether the respondents understood the question. 35.5% of the respondents (38) also answered the follow-up question "What is the primary reason for your score?". These comments were to the point and insightful, it is clear that the question was understood.

A sample of these comments is in Table 5.

Score	Comment	Group
3	Have not obtained security documents	Lack of knowledge
4	No idea what safeguards are in place. We just have to trust.	Lack of knowledge
8	https and overall good application	Argumented
8	sometimes I feel that access control may not be good,	Control
8	GENERAL FEELING	Other

Table 5 A sample of answers given to the follow-up question in the security perception survey.

There were 14 comments that were very generic like the last sample in Table 5. Rest of the comments are mostly written in the form of "something could / should be improved further" and the comments belong to four groups:

- Possibility (Previous incident) - respondent had had a security incident with the app some time ago

- Lack of knowledge - the respondent is unsure and feels that additional information about security measures is needed

- Control (request for a security measure) - respondent brought out a specific security measure missing

- Augmented - the respondent has the reasoning of why they think they feel confident with the product security

Such comments had both low and high ratings from the respondents.

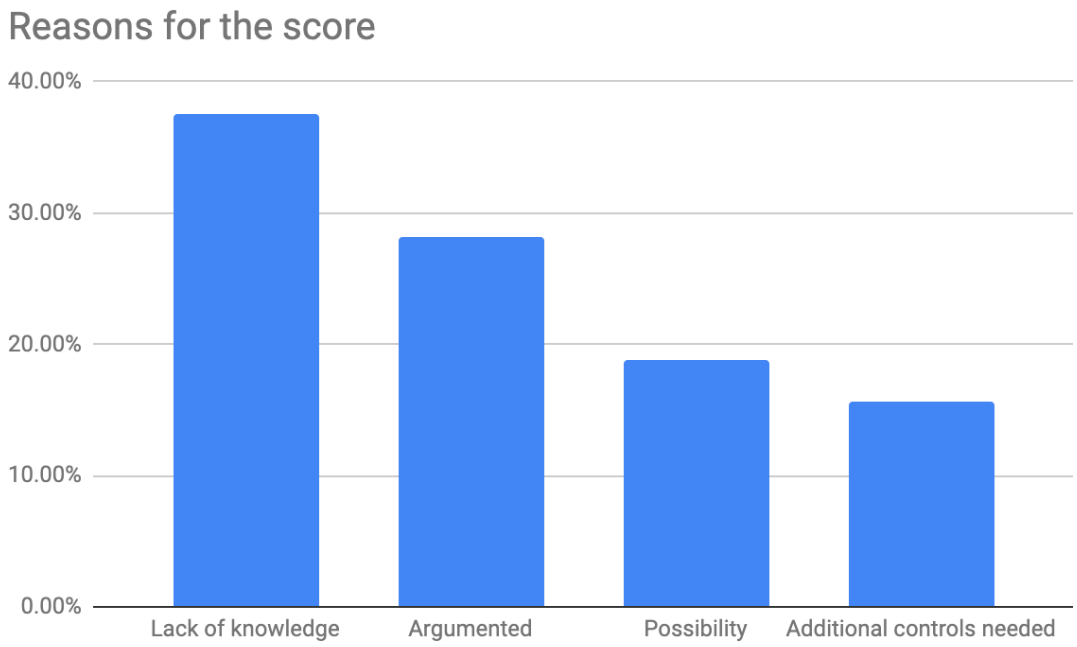

Figure 9 Respondents answers grouped to categories which would need improvement to increase that respondent's perception of security score.

For further analysis, the responses with comments were grouped into six KISCAP clusters based on which of the six factors should be either increased or decreased in order to improve that respondents score. The generic comments like *"general feeling", "gut feeling"* were categorized into *Other* group as the required steps to improve the scores for these responses were not that obvious. The author believes that such generic scores could be impacted by steps taken in a number of the KISCAP categories.

The groups are visualised in a radial graph in Figure 10 Survey responses grouped into KISCAP clusters. The value represents the number of comments in that category.

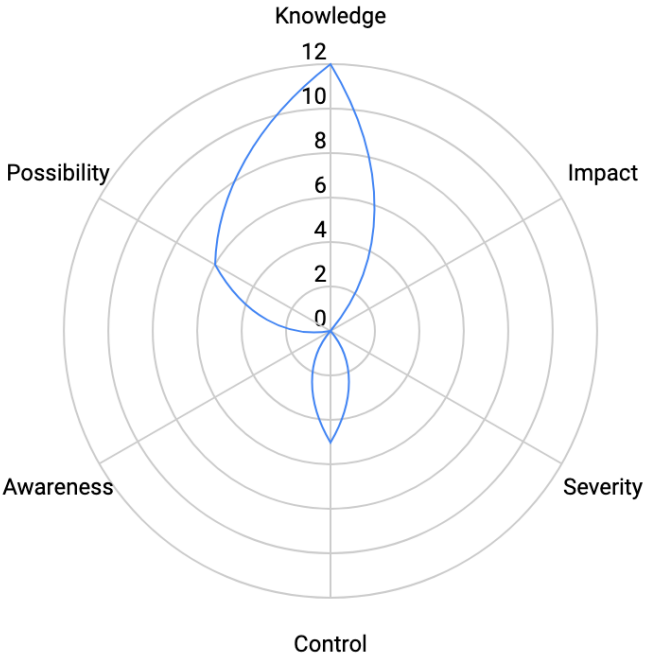

Figure 10 Survey responses grouped into KISCAP clusters. The value represents the number of comments in that category.

From the comments, three main groups stand out - knowledge, controllability and possibility. The context of the survey was to evaluate B2B applications security not a specific threat as in the original KISCAP research. Therefore, it is understandable that severity and impact did not get mentioned much, as these would be more applicable categories for assessing specific threats (as in the original KISCAP paper).

Looking at the sentiment of the comments, then scores from 0 to 4 were rather negative, often mentioning a previous security incident; 5-s were quite passive, and scores from 6 to 8 were more positive. Interestingly, none of the scores of 9 and 10 answered the follow-up question. This matches with how respondents are clustered in the NPS survey - detractors, passives and promoters. It is probable that if a similar question about this products security came up in real life of the respondents, then the admins who gave the score from 0 to 4 will not be recommending it and respondents with scores higher than five will probably have a few kind words to say like they did in this survey.

As the sentiment aligns well with the NPS framework, there are grounds to analyse the results through detractors and promoters and calculate the “Net Promoter Score for the products’ Security”. The result, however, is unfortunately lower than the 45+ expected by the stakeholders. Considering that the overall tone of all the comments is focusing on

improvements, the author believes that it would be difficult to reach the highest quintile of the NPS score (+50 and beyond). With some investments in to the area, it would certainly be possible to achieve a positive score around 30-40 for more generic SaaS products that are not focusing specifically into security where the expectations to the extent of the security features will be much higher.

Based on the KISCAP analysis, in this case there is most opportunity to improve the security perception score in raising the knowledge factor. Informing users more about existing security measures of the product, creating transparency into who of products employees and customers fellow employees can see and modify data; in which country the data is stored *etc*.

The first results of this survey got a good reception from the stakeholders as the product team saw value in the input and were able to make decisions based on the entire framework. Based on the emergence of the Knowledge category as the most significant one, it was decided that in addition to customer facing security feature development additional emphasis will be put into educating customers about existing security measures. This means additional customer communication about existing security features is a key part of the next quarter plans for the team.

A more throughout analysis of the stakeholder reception of the first survey results and use of this framework will be done in the following chapter.

4.2 Analysis of the perception of security metric

4.2.1 The target group of the metric feedback

After the first perception of security survey results were gathered from stakeholders and other employees of the company. At the beginning of the survey, they were given a brief introduction about the challenges of measuring the ROI of security features and research showing that the perception of security impacts the adoption of web services. The goal of the survey was to understand whether the metric is clear to stakeholders, what they thought the value of security perception score we should aim at and how they rate the metric itself as the most important metric for the team who is responsible for developing customer facing security features.

Feedback was collected from 3 different groups of employees. The total number of respondents was 40 which is 8% of the total number of employees. Table 6 displays the group label and the job titles grouped into the group based on the survey respondents responses.

Group label	Job titles in the group
Executive team	CEO, CTO, VP of Engineering, VP of Product, Head of Core Product
Managers	Design team lead, Engineering manager, Head of research, Lead Product Manager
Specialists	Developer, Backend developer, designer, product data analyst, customer support, support engineer, customer solutions expert

Table 6 The group label and the job titles grouped into the group.

In addition, all the respondents were categorised based on whether they work in the team responsible for developing the security features and whose team KPI is the perception of security. This was done due to the possible bias from the team closely working on developing and improving the metric.

4.2.2 Feedback analysis

The following analysis will explore two topic areas. First, what are the expectations of stakeholders and other employees of the company on what the security perception score for their product should be. Secondly, what are their thoughts about the security perception score and the framework overall.

- The expectation of what the perception of security score should be

Figure 11 Breakdown of scores of the expectation of what the perception of security score should be

All respondents found that the perception of security needs to be higher than 7, 95% expected the score to be even higher than 8.

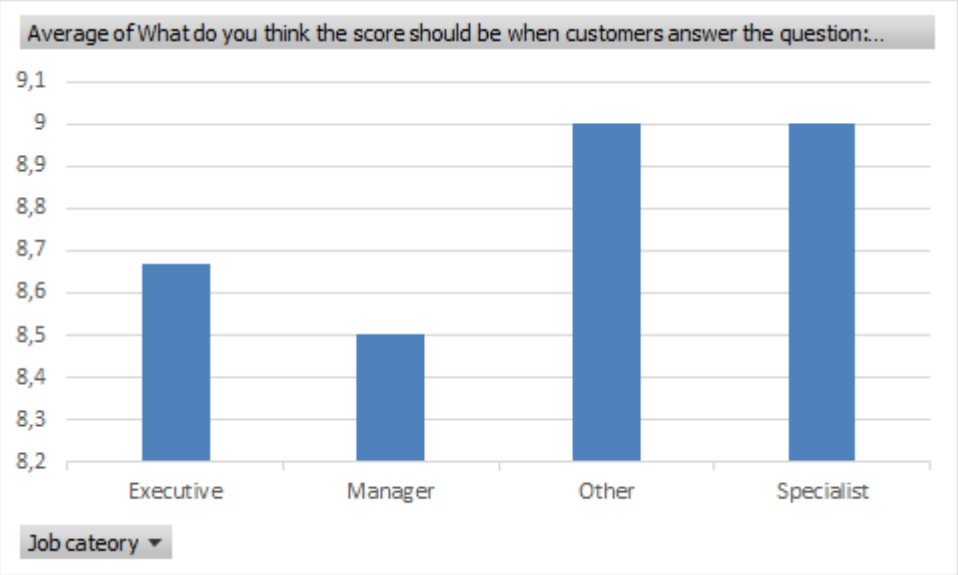

Figure 12 Breakdown of average expected scores by different job categories. In this chart product related specialists and other specialists were broken into two groups to see if there were any differences between them.

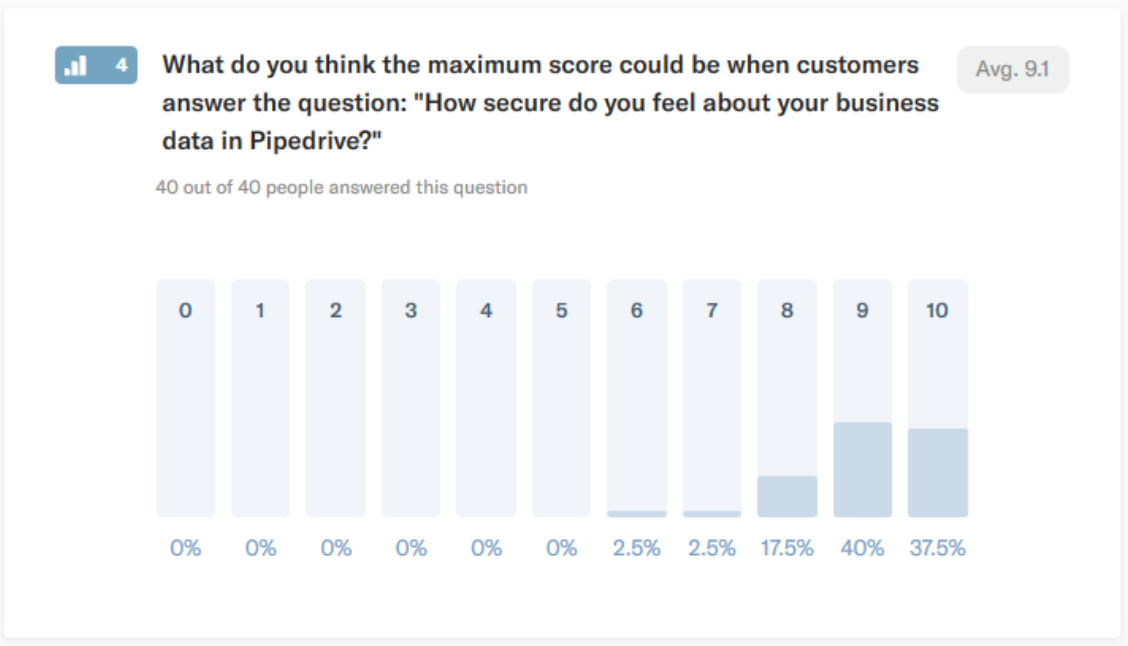

Figure 13 Breakdown of estimation of the theoretical maximum perception of security scores that could be achieved.

From the respondents, the executive and manager roles had lower expectations of what the score should be. This can be due to experience with different KPI-s and their individual interpretations of what the score maximum could be. When compared to the answers of what the maximum of such a score could be, then this confirms that the executive and management team members expect the maximum to be lower as well, compared to specialists. Although, here executives' expectations are very close (9.3) to specialists (9,4) the manager's score (8.25) is significantly lower.

Overall the average expectation across all roles was 9.

The expectation of the score to be over 8, was confirmed in the answers to another question - *"What do you think, at what score the investment to the security features could be decreased?"*. The average score to that question was 8.5 and 89,6% of respondents choosing options above 8.

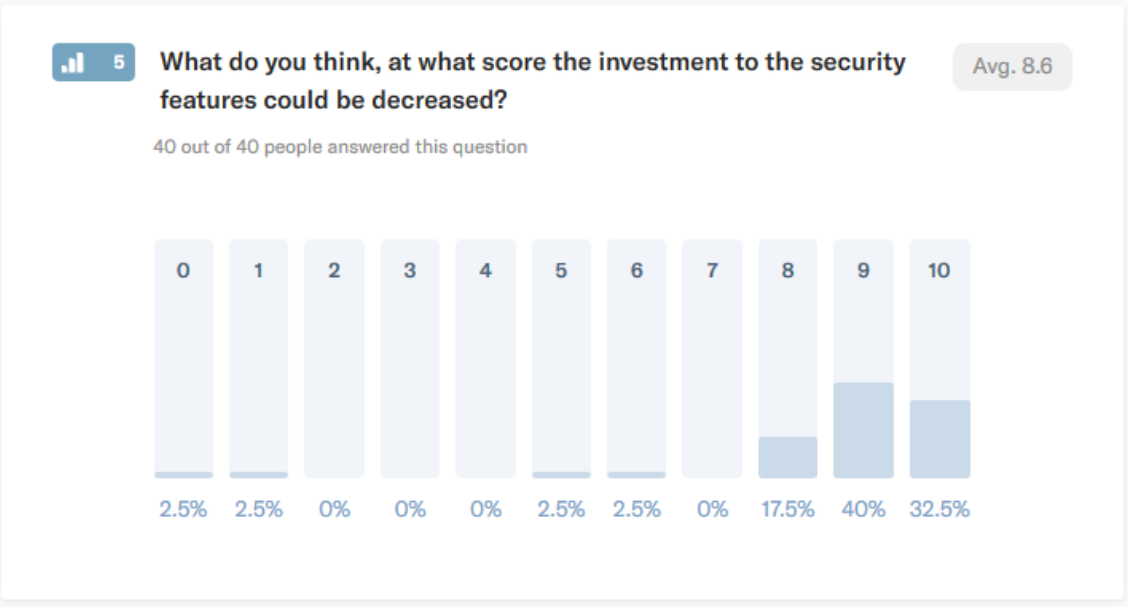

Figure 14 Breakdown of responses when the investment to the security features could be decreased.

- Estimations of what the perception of security was in the test survey

When estimating how the users actually rated their perception of security 84,6% of responders estimated it to be lower than 8. At the same time, 93% stated that the score should be higher than 8.

Figure 15 Breakdown of customers perception estimations by all respondents.

Figure 16 Breakdown of customers perception estimations grouped by job category

When estimating the actual score given by the users, Managers remain to be the most conservative group - expecting the score to be 5.8 which is significantly lower to Specialists (6.4) and Executive 7.0 score.

Answers to questions analysed so far, give a clear indication that the security perception score for this particular SaaS product should be over 8. The first survey also showed that scores from 6 up were more positive and scores higher than 8 did not even have any comments. Considering that even at higher scores, most of the comments were about things that needed improvement, score over 8.5, indicates customer satisfaction. The author argues that aiming at a security perception score of 8 or more is a safe goal which should satisfy customers in different sectors and expectations. However, the goal could also be set lower. How low exactly, could be derived from the first security perception score by looking at which score the negative or suggestive comments stop.

On the other hand, in an industry where customers share less sensitive data, their perception might be proportionally higher already. This would require further research to be done in measuring the security perception of different products.

- Rating for the metric - *"How satisfied are you with the concept of security perception score as the North Star metric for a team working on security features?"*

The question mentions "North Star metric", it is a term widely used in the company for the one most important metrics each team in the company has and is working towards improving. Most of the teams efforts should go towards improving this one "North Star" metric. In other companies such a metric is often called Key Performance Indicator (KPI). Although the term is used often in the product teams of the company, it was revealed that for some people in other roles it was unfamiliar and due to that they were not able to answer the question adequately. These three ratings (2 times 5 and one 1) were removed from the results.

80% of the responders rated the metric with a score of 7 or higher. The explanations for the lower scores were due to not understanding the goal the score aimed to serve. The aim was to measure the perception not the actual secureness of the product as some respondents mistakenly thought and therefore found it to be not the best metric. On average the executive team was most satisfied with the metric with the average score of 8.5, the Managers rated it with 8.25 and the Specialists 7.25. The low score from the specialist can be due to the fact that the perception of security is quite an abstract concept and it is not very clear to the specialist if and how they could contribute to the score. The main stakeholders and audience for the score are the executive team and the managers who based on team's North Star metrics grade their performance and decide on future investments to the area. The main stakeholders were satisfied with the concept of the metric which is very good, as one of the early motivations of researching this topic was to find this single metric.

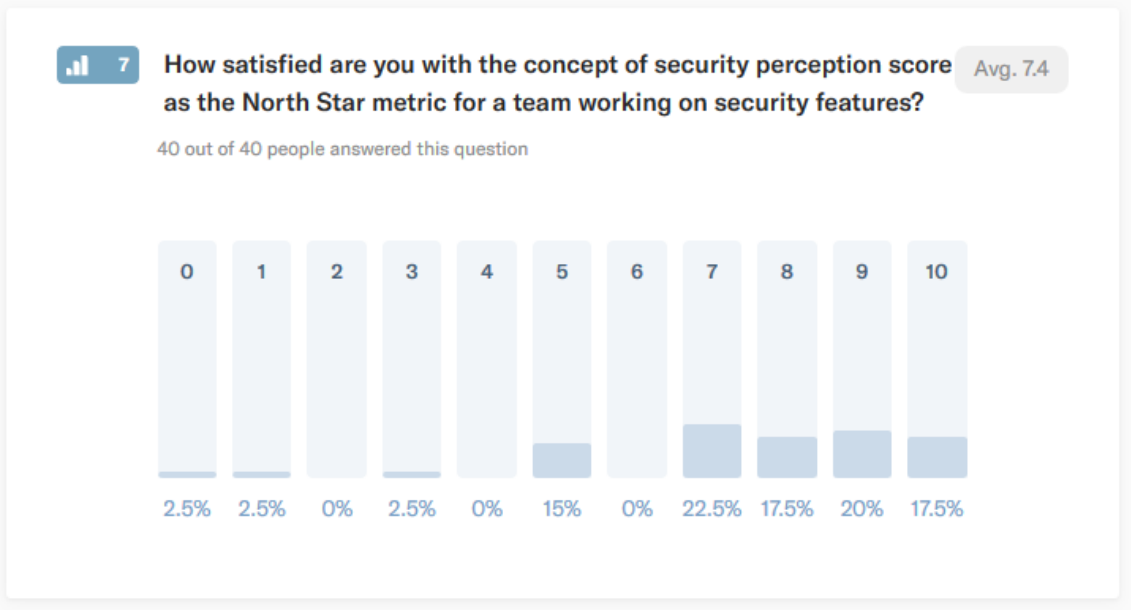

Figure 17 Breakdown of respondents' satisfaction with the perception of security being the key metric for a team working on developing security features.

This rating also had a follow-up question *"What is the primary reason for your score?"* displays some of the answers to this question.

Score	Comment	Job category
10/10	I think it makes perfect sense to measure it like this	Manager
8/10	A security perception is great as a sales driver, but I'm not 100% sure it should be the North Star. Only 80% sure :)	Manager
7/10	Perception is not the same as the reality. Though, it is difficult to measure how secure something really is	Specialist
7/10	I am more into actual security than just what customers think of it	Specialist
9/10	Customer perception combines actual security and understanding of security measures by the customer. Both are important	Executive
8/10	Perception is important but we should look at the actual security incidents and metrics as well	Executive
7/10	I can't think of a better one right now, hence I'm positive, especially if our survey is recent. I will say, though, that for me security perception is the result of features (product), actual reliability (infra), and messaging (marketing). All these should be part of and have an impact.	Executive

Table 7 A sample of answers to the follow-up question to understand the primary reason for their score given to "How satisfied are you with the concept of security perception score as the North Star metric for a team working on security features?"

- Rating for the format NPS vs 10-point scale

Due to a technicality, this question was marked as optional at the beginning of the survey, and some of the respondents did not answer this question.

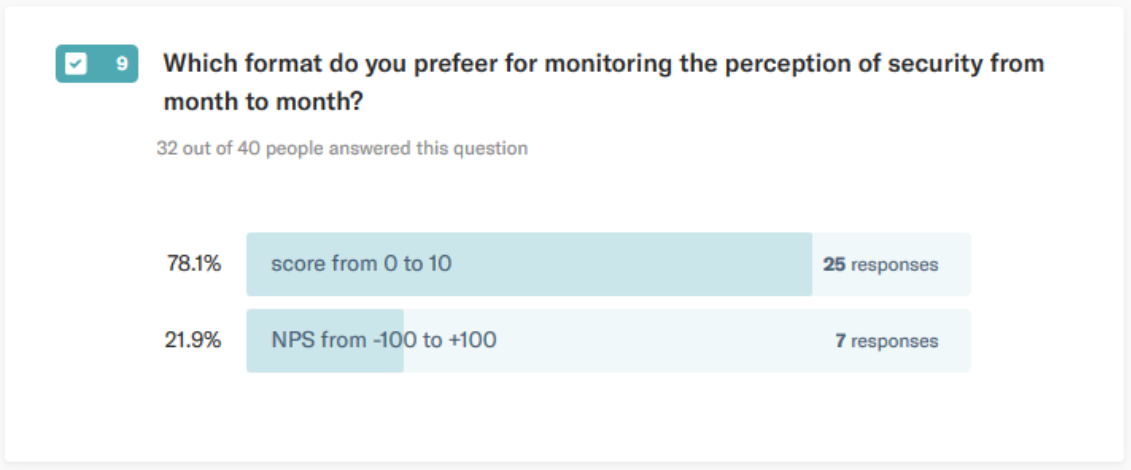

Figure 18 Breakdown of respondents' preferences on representation of the security perception score

Using the NPS framework, made it technically easy to conduct the survey. The tools were already there for customers to give 10-point scale ratings without leaving the app. Putting together the survey was less time consuming as well. We were able to use in-app communication through *Intercom* which already had all customers information and made it simple to target and contact the customers. Alternative ways would have required us significantly more effort to gather the target group contacts, designing and composing emails and the survey interfaces.

A vast majority of the respondents (78.1%) however preferred the 0 to 10 format as the metric over NPS. Looking at the roles of respondents preferring NPS format - these were roles closer to product management - product managers, product designers *etc*. Surprisingly, a few people brought out that the reason why they did not like NPS was since the NPS score from the first survey was "alarmingly low" (Maria Angelina Lasprilla Mejias, Head of Core Product). The score in 10-point scale, however, was "mediocre enough to spark action" (Maria Angelina Lasprilla Mejias, Head of Core Product) but not too "dramatic" (Jana Krivorotko, Lead Product Manager).

Product manager working in the security features area, who tested the framework out for a few months stated that: "Although NPS format is more informative, the 10-point scale is easier to talk about with people in different roles who might not be that familiar with the NPS and how exactly it is calculated" (Madis Sulg, Product Manager). All executive team members surveyed (CEO, CTO, VP of Engineering) also preferred the 10-point scale format.

Therefore, the best solution for all parties is to take advantage of the tools built for surveying NPS when conducting and analysing the survey results but share the simple 10-point scale average score with stakeholders.

4.3 Analysis of the prioritisation framework

The development of this framework started because of a need to quantify the work that is done in the security features area of the product. Although there was an understanding of the conceptual importance of the field, the question - *"Should we continue with the full team and for how long?"* still came up too often and was very difficult to answer. The answer was never definite, but rather yet another discussion and explanation of the conceptual importance of developing the security features.

Although it might seem like this is either an internal challenge in one company or something that could have been already solved universally within the industry then unfortunately this is not the case. There did not exist a framework (or at least not a widely known one) for measuring the impact of customer facing security features that could be used for prioritisation. In the authors experience of working as a software and hardware product manager in four companies over 10+ years the need for such a framework has been there in all of them. Without such a framework it is very difficult to get the stakeholder understanding and buy-in needed for continuous investment into developing customer facing features (there of course can be exceptions where the stakeholders have strong cyber security understanding and mindset).

Once the security perception score was figured out in the company where the framework was tested, and the first results were in, the rest fell into place as well. The security perception score makes it clear why work needs to continue in the area. The understanding of what impacts the perception of security among the customers helps to understand why the features that the team is working on were chosen compared to other options. Using the developed model in the customer feedback analysis and seeing the potential that good customer communication can have, made it clearer which types of activities to prioritise and emphasised the understanding that security perception can never be a responsibility of one product team. Maximising it is a joint effort between product, product marketing and information security teams. This shared understanding

made the importance of cooperation between these teams clearer and gave it more priority from the stakeholders as well.

In addition, positive feedback from the stakeholders showed that the perception of security score can not only be used as a metric for measuring the impact of security features development but also can serve as a key metric for the teams responsible for developing such features. As one stakeholder brought out the perception of security score will be a joint effort between multiple teams. The author argues that this is the case with many key metrics. For example, often additional revenue is used as a key metric for teams, which also in reality will never be a result of one individual team or effort. Therefore the perception of security score is as suitable to be a teams' key metric. The perception of security framework is now fully adopted in the company for measuring the impact of security feature development (and other activities) and prioritising related activities. There is also an agreement that the investments will not decrease until the perception of security score is consistently over 8.5.

5 Summary

In most cases, the reasonable approach for small and medium enterprises (SMEs) is to use Software as a Service (SaaS) applications hosted "in the cloud" instead of developing and maintaining in-house software for business processes where cloud software is available. Ease of management, however comes with a price. Customers often have no visibility into what data is accessed by whom, where and for what activities. Customers need to put a lot of trust in the providers to mitigate the risks transferred to them and make the right investments in security. Data security in the cloud is seen as the primary risk companies are facing today [1].

The conceptual importance of data security for customers has been often demonstrated [1], [3], [6]. There, however, is no framework for understanding the return of SaaS Security investment which is crucial to justify investing in such feature development and understanding whether the investments should be stopped, decreased, continued or increased. This is with paramount importance in order for teams to be able to increase the security of customer data in software products.

In this thesis the author compared ways of measuring the impact of developing security features to business-to-business (B2B) SaaS products that would be applicable to both potential new and already existing customers with as little bureaucratic burden as possible. Measuring customer's perception of security was selected as the most suitable metric as opposed to trying to calculate the potential loss reduction of every customer, counting incidents related to security measures of the product or trying to calculate the additional revenue earned or lost due to security measures.

Next a framework was developed to support the surveying of the perception of security score and help in prioritising activities that would have the greatest opportunity to increase the score. This in turn would support the product growth either through new or expanded revenue from existing customers.

A two question survey with a 10-point scale rating to the question *"How secure do you feel about your business data in service X?"* and a follow-up question *"What is the*

primary reason for your score?" was developed as the method for measuring the perception of security score. Using existing tools for Net Promoter Score surveys, widely used by product companies, was suggested as the technical means to conduct the survey due to familiarity and ease of adoption.

Next, the author built upon existing research by *Huang et.al.* [2] [10] into the factors impacting the perception of security and their impacts on IT adoption and security practices. The author proposed a novel new way of how the same six-factors (KISCAP – Knowledge, Impact, Severity, Controllability, Awareness and Possibility) proposed by *Huang et.al.* [2] could be interpreted in software product management for categorising and prioritising improvement activities to maximise the perception of security score. The framework together with the factors, their impact to the perception of security and the growth through new customers or expanded revenue from existing customers is visualised in the following Figure 19.

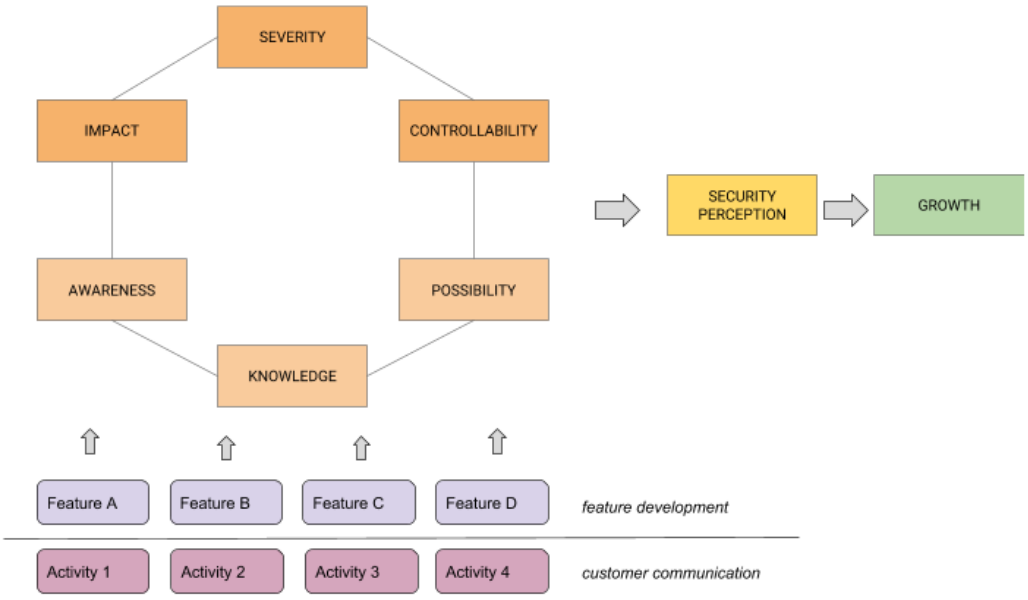

Figure 19 The framework proposed by the author of how the perception of security develops and how it impacts the security perception score and growth through revenue from new customers or expanded revenue from existing customers.

Finally, the developed framework was tested with a B2B SaaS application, the survey results and feedback from the stakeholders was collected and analysed for further improvements. As the result of this test, the perception of security framework is now adopted in the company for tracking impact, prioritisation and for deciding until when the investments into developing security features should continue as they are now.

The test of the framework and following analysis showed that:

- the perception of security framework is a well understood and received framework by stakeholders including executive teams
- the perception of security score can be used to quantify the impact of security features developed into a SaaS application;
- the perception of security is suitable to be the most important metric for the team that is responsible for developing customer facing security features;
- the perception of security score can successfully be used to decide whether enough security measures been implemented or should investment into the area continue if not even be increased;
- the Net Promoter Score framework of detractors and promoters is a good way to analyse the results of the survey but the simple 10-point scale should be used in discussions with stakeholders by whom that scale is more understandable and preferred;
- that a generic software product (not a cyber security specific product) should aim to reach a security perception score of 8.5/10;
- the six KISCAP factors can also be interpreted in product development for finding and prioritising the biggest opportunities for improvement in customer facing security features area;

This, however, is just the beginning. There are still aspects of the framework that need further research. The framework needs to be tested with more products in different segments and with different business models to understand how much the perception varies naturally within one product over time and between different services. Does the perception of security of customers vary based on the level of confidentiality of data stored in the application? Time and experience will also help to answer the question what is the maximum security perception score that could be achieved and how much different activities can impact the score within a short and over a more extended period of time.

References

[1] M. Raskino, “Gartner,” Gartner, 6 April 2018. [Online]. Available: https://www.gartner.com/doc/3870869/-ceo-survey-cios-guide. [Accessed 20 April 2019].

[2] Huang, Ding-Long; Rau, Pei-Lueng Patrick; Salvendy, Gavriel; Fei Gaoa; Jia Zhoua, “Factors Affecting Perception of Information Security and Their Impacts on IT Adoption and Security Practices.,” *International Journal of Human-Computer Studies,* vol. 69, no. 12, p. 870–83, 2011.

[3] J. Metsamaa and T. Pihl, “Big Team Research,” Pipedrive, Tartu, 2018.

[4] European Network and Information Security Agency, *Introduction to Return on Security Investment,* 2012.

[5] “Wikipedia,” Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Alexa_Internet#Alexa_Traffic_Rank. [Accessed 8 May 2019].

[6] D. Ene, 2checkout, 6 April 2017. [Online]. Available: http://blog.avangate.com/review-directories-for-listing-software-saas-products/. [Accessed 8 May 2019].

[7] Q2 Crowd , “Best Software Companies 2019,” 2019. [Online]. Available: https://www.g2.com/best-software-companies. [Accessed 8 May 2019].

[8] D. Cooper, “Psychology, risk and safety. Professional Safety,” *Professional Safety,* vol. 48, no. 11, pp. 39-46, 2003.

[9] B. Suh and I. Han, “The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce.,” *International Journal of Electronic Commerce,* vol. 7, no. 3, pp. 135-61, 2014.

[10] Huang Ding-Long, Pei-Luen Patrick Rau & Gavriel Salvendy;, “Perception of Information Security,” *Behaviour & Information Technology,* vol. 29, no. 3, pp. 221-32, 2010.

[11] “TOP7,” TOP7.io, [Online]. Available: https://top7.io/customer-service/nps-tools. [Accessed 20 April 2019].

[12] F. F. Reichheld, “The One Number You Need to Grow,” *Harvard Business Review,* vol. 81, no. 12, pp. 46-54, 2003.

[13] CustomerGauge, “NPS Benchmarks,” [Online]. Available: https://npsbenchmarks.com/blog/4-key-ingredients-fuelling-apples-high-net-promoter-score. [Accessed 20 April 2019].

[14] C. Gocheva, “NPS Benchmarks,” CustomerGauge, [Online]. Available: https://npsbenchmarks.com/blog/4-key-ingredients-fuelling-apples-high-net-promoter-score. [Accessed 20 April 2019].

[15] B. Chudoba, “Curiosity at Work,” SurveyMonkey, [Online]. Available: https://www.surveymonkey.com/curiosity/survey_questions_and_completion_rates/. [Accessed 11 May 2019].

[16] R. P. a. S. R. B. Curiel, “A Metric of the Difference Between Perception of Security and Victimisation Rates,” *Crime Science,* vol. October, pp. 1-15, 2016.

[17] “Cost–benefit analysis,” Wikipedia, 2019. [Online]. Available:

https://en.wikipedia.org/wiki/Cost%E2%80%93benefit_analysis. [Accessed 20 April 2019].

[18] D. F. Austina De Bonte, Scenario-Focused Engineering: A toolbox for innovation and customer-centricity, 2014, p. 249.

[19] "Survicate - Where leading teams collect and act on customer feedback," [Online]. Available: https://survicate.com. [Accessed 20 April 2019].

[20] "Intercom - Customer Messaging Platform," [Online]. Available: https://intercom.com. [Accessed 20 April 2019].

[21] C. STAMFORD, "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019," Gartner, 12 September 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019. [Accessed 21 April 2019].

[22] K. Panetta, "Smarter With Gartner," Gartner, 27 May 2018. [Online]. Available: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/. [Accessed 20 April 2019].