15/09/2017

THE ROLE OF RATIONALITY

– A Stakeholder Management It-security Case Analysis of Rationality in Decision-Making

080591-XXXX | Rasmus West Nordskilde | Copenhagen Business School
|Characters: 176.785 | 72 pages |

Abstract

To obtain efficient stakeholder management, it is needed to have an understanding of decision-making. Among the concepts affecting decision-making is rationality, and therefore it is important to know the role of rationality in decision-making. To understand the role of rationality in decision-making, the thesis has done a case analysis of it-security. The case of it-security was chosen as a general example of decision-making, because it was seen as being able to showcase an examination of the theoretical concepts of rationality. The results of the analysis pointed to ecological rationality as best describing the role of rationality. Thereby the analysis suggests that decision-making is largely rational, but within boundaries of limitation. The non-rationality concepts rather came to deliver comfort after satisficing had been conducted. This leads to the need for further studies on how to best take precautions of ecological rationality when executing stakeholder management. To give perspective to the conclusions, it was recommended to expand trials on nudging, where specific attention was put on circumventing opposing ecological rationalities.

Contents

Introduction

The world of the decision-makers in the 21st century is more digitalized than ever. The internet is being connected to everything, and over a relatively short time span, as shown in figure beneath, the number of devices connected to the internet, called IoT-devices, will greatly surpass the population on earth:

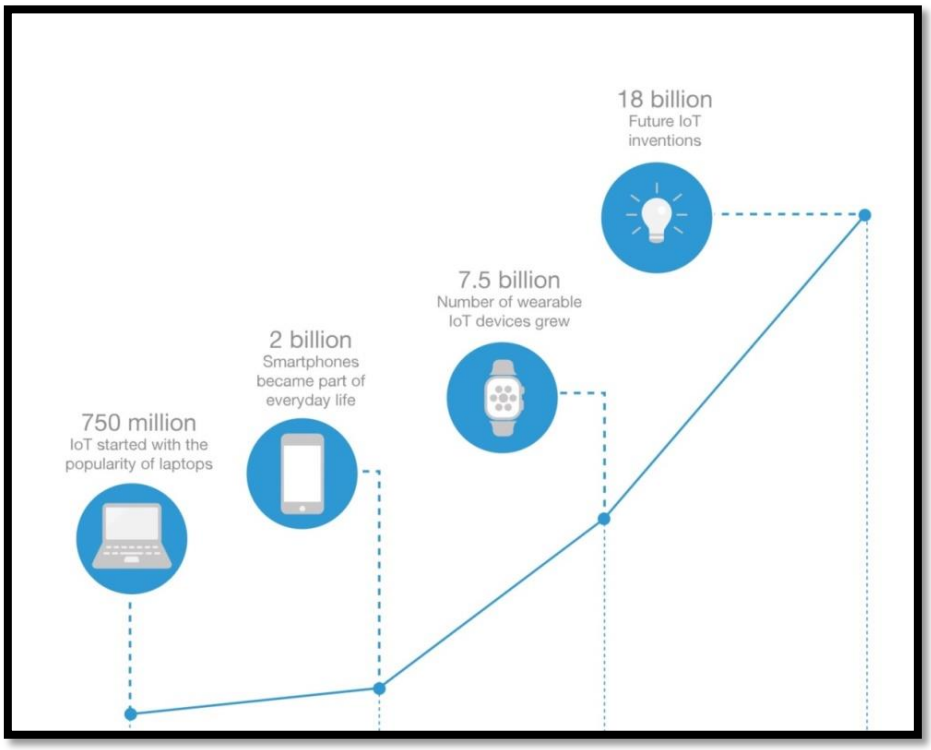

Figure 1: Internet of Things, Tado, 2017. Available at: https://www.tado.com/sg/internet-of-things

Among the decision-makers, who has to maneuver in the digitalized world, is the consumers and citizens. Both groups are central actors within society, and on each their platform, consumers and citizens are the central decision-makers. On the market, consumers are the counterpoint to the sellers. The citizens are on the other hand the decision-makers within the state. Both groups combined constitute a massive group of decision-makers, and a group of decision-makers that are individually making decisions on their own behalf.

The digitalization has unfortunately also affected the way consumers and citizens become victims of crime. Theft in the 21st century is centered not only on physically valuable items, such as bikes, cars or smartphones, but also on digital fraud. The becoming of the types of digital fraud is

increasing with the new possibilities within the digitalized world. The growth of digital fraud is happening in contrast to the last decade in Denmark that saw a steep decline in theft crimes[1].

Unfortunately, digital fraud is an exception to this development, because as the world develops, so does the world of crime. New opportunities arise and new forms of crime are being explored. Digital fraud, as the digital version of an "intentional perversion of truth"[2], is about gaining access to the devices or private information of the consumers and citizens. This is later used to blackmailing or install malicious software collecting personal information such as credit card information and bank details.

Background

Looking generally on fraud from 2015 to 2016, reports instigate that fraud in Denmark grew with 25%[3]. The main factor is the becoming of digital fraud, which has proved to be too big of a task to prevent. Looking at the most recent numbers from Statistics Denmark, the emerging rate of digital fraud is nothing short of frightening:

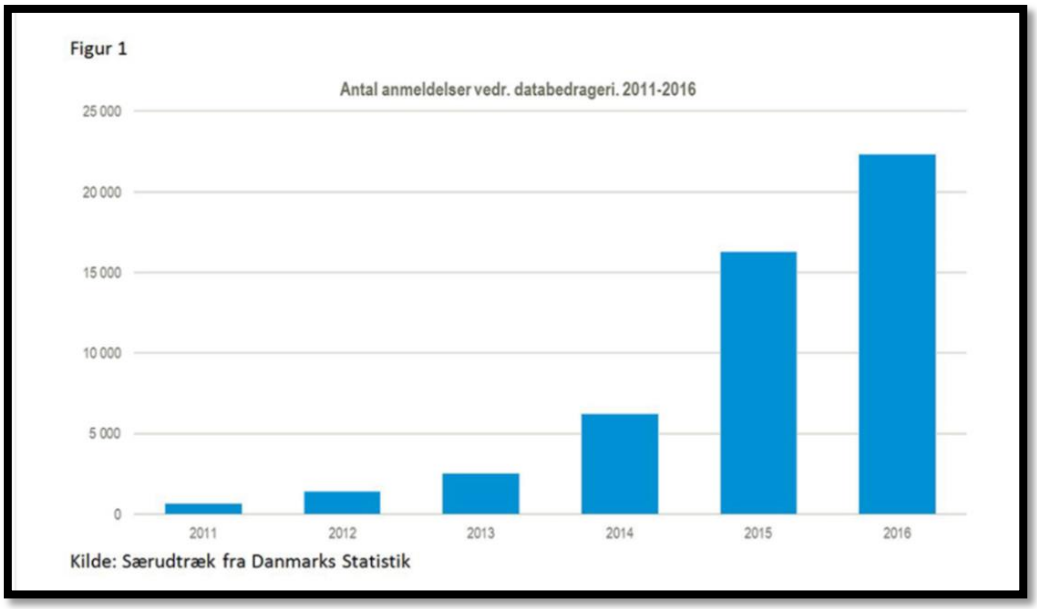

Figure 2: Flere databedragerier still krav til brugernes it-sikkerhed, Danmarks Statistik, March 2017. Available at: http://www.dst.dk/da/Statistik/bagtal/2017/2017-03-27-flere-databedragerier-stiller-krav-til-brugernes-it-sikkerhed

[1] Fra barndommens gade til cyberspace, Flemming Balvig, Det Kriminalpræventive Råd, 2017, p. 14
[2] Fraud, Merriam-Webster Dictionary.
Available at: https://www.merriam-webster.com/dictionary/fraud
[3] Flere bedragerier, færre brud, Danmarks Statistik, February 2017.
Available at: http://www.dst.dk/da/Statistik/nyt/NytHtml?cid=23527

As the figure above shows, with only 647 cases in Denmark being reported to the police in 2011, compared with the overwhelmingly rise to 22.339 reports in 2016, the increase in reported cases of digital fraud has roared with 3452% in only 5 years. That is more than a thirtyfold increase in only half a decade. This rapidly growing sector of digital fraud is covers among other things false e-mails, competitions, texts, links and phone calls, but also violations of copyright law and malicious software. What all digital fraud share is the goal of illegally attaining value from the consumers and citizens. This new technological development of digital fraud has started a race between it-security and it-criminals, where the latter in recent years have had a boom in activity according to reported incidents.

Digital fraud is due to this an area of special concern to stakeholder managers on the field, including public institutions, private companies and NGOs. The most frequent way to tackle the increase in digital fraud has so far been by giving advice, where stakeholder managers have designed workshops, pamphlets and campaigns to increase awareness among consumers and citizens. The messages have focused on more or less the same features, and always include a combination of skepticism, digital know-how and safeguarding[4,5,6]. Among them are often five key elements to improve it-security:

- Do backups
- Install antivirus
- Update devices
- Have a healthy skepticism
- Use unique passwords

Those advices, according to different experts and sources, would – if systematically and consequently followed - heavily increase it-security of consumers and citizens. Nevertheless, a majority of the Danish citizens and consumers do not follow the advice given[7]. Seemingly going against all rationality, the consumers and citizens do not take to them the suggested initiatives to prevent digital fraud, resulting in digital fraud not being met with a reasonable countermove. This

[4] 10 råd til sikker pc-brug, Digitaliseringsstyrelsen.
Available at: https://www.borger.dk/internet-og-sikkerhed/Sikker-selvbetjening/Se-10-gode-raad
[5] 10 gode råd til bedre sikkerhed, C-Cure.
Available at: https://www.c-cure.dk/for-private/10-gode-raad-til-bedre-sikkerhed/
[6] 10 tips til bedre IT-sikkerhed, Ekstra Bladet, Thomas Gösta Svensson, Anders Ejbye-Ernst, Alexander Sokoler, Steffen Moses og Jens Christian Hillerup, August 2015.
Available at: http://ekstrabladet.dk/nyheder/friadgang/guide-10-tips-til-bedre-it-sikkerhed/5698949
[7] Trendrapport 2016, DKCERT - DEIC, different authors, 2016, p. 12

leaves stakeholder managers will the conundrum of not being able to change the behavior of the stakeholders they are trying to manage.

Purpose of the thesis

The seeming lack of rationality in the decision-making exemplifies how the deliberation behind decision-making continues to be a mystery. If the underlying reasoning of decision-making was known, the strategy of the stakeholder managers, based on the advice of it-experts, would be formulated, spread, taught and constructed differently.

In the case, it is clear that rational steps, according to it-experts, are not finding an audience among consumers and citizens. In order to understand how stakeholder managers can hope to affect consumers and citizens to a higher degree, it is therefore fruitful to conduct an analysis of rationality in decision-making. Without an understanding of how rationality resides in decision-making, it is futile for stakeholder managers to put forward initiatives that will have an effective impact. Therefore an analysis of rationality in decision-making is not only relevant to the current example of it-security. The keynotes will be able to give insight to the role of rationality when generally conducting stakeholder management in a broad range of situations.

This is done by using the case of it-security to shed a light on the different aspects of theory concerned with rationality in decision-making. The perspectives of the case will be used to support analytical points in the discussion of decision-making with or without rationality as a key component.

The lacking engagement of consumers and citizens to follow the advice of it-experts will be used to shed light upon different aspects of the theories. The focus will be on whether concepts including rationality, such as bounded rationality, satisficing and ecological rationality, can explain the behavioral patterns, or if theory excluding rationality more accurately contributes to the understanding of decision-making.

The findings will therefore not be attributed to solely to it-security. Rather, the conclusions of the thesis aims to more broadly highlight the role of rationality in decision-making. The case of it-security is solely used as the canvas upon which an analysis of rationality and non-rationality

theories of decision-making can be portrayed. The consumers and citizens serves in the role of decision-makers, and thereby as a representative of decision-making.

The following research questions will be answered upon the finalization of the thesis:

1. *What role is rationality playing in decision-making of stakeholders, and how is rationality best considered in stakeholder management deliberations?*
2. *Can rationality theories of bounded rationality, satisficing and ecological rationality better explain decision-making, than non-rationality theories of decision-making focusing on mental accounting, overconfidence, prospect theory, cognitive dissonance, emotions and choice architecture?*

The combination of portraying a discussion of behavioral economics theory on the symbolic case of it-security, based on expert interviews, articles and reports, contributes to expanding the knowledge on how politicians, NGOs, and others need to consider rationality within stakeholder management.

Delimitations

- The thesis aims to be able to more broadly conclude on decision-making, but the case is based solely on consumers and citizens in Denmark.
- The analysis is based upon five pieces of selected advice. These could have been prioritized differently, but the composition chosen is done in order to best portray a multitude of angles on the case of it-security, and also due to these specific pieces of advice common recurring.
- The theory has been sharply divided into definitions of rationality and non-rationality concepts. This division is beneficial to the analysis, but will limit the degree of flexibility to discuss fluctuations between the concepts.
- To highlight theoretical points the best possible way, the decision-maker will through the thesis be symbolized by consumers and citizens. These groups do not cover all decision-makers, but they are valid representatives of decision-makers, seeing as they in different fields cover a wide array of decision-making.

- It is the governing and strategizing of decision-makers that constitute the backbone of the thesis. Therefore the conclusions are not aimed at decision-makers, but instead the stakeholder managers who are concerned with the behavior of decision-makers.
- The thesis is based on whether or not ignoring advice on it-security by consumers and citizens is rational. Thereby the thesis does not engage in discussion on the concept of rationality itself.
- The report has been conducted on the basis on interviews of two experts on the field of it-security, several reports on it-security and theory acquired from behavioral economics theory. This combination gives certain insights, but with limited length of the thesis, along with a limited time span, relevant knowledge from other fields of theory and empirical data had to be excluded.

Methodology

Research Setting

Problem area

The thesis is based on a discrepancy within the field of stakeholder management and behavioral economics. In behavioral economics there are different theories on decision-making. Some lay more credit to rationality than others. It is this role of rationality in the field of decision-making theory that is the general setting for the thesis. Following this problem area, it is stakeholder managers who by more inclusively understanding the role of rationality in decision-making hopefully will be able to gain valuable insights.

Approach

In order to get the theoretical discussion portrayed, the case of it-security was introduced. By introducing the case of it-security, the analysis was able to more relevantly test and asses the different assumptions within the chosen theory. The case thereby puts theory to the test, thus functioned as a way for points to be made clear, and as a way of supporting or opposing assumptions and conclusions within the theory. The analysis of rationality in decision-making is not aimed on delivering answers purely on it-security, but rather to give insights on a broader level of decision-making. This means that the conclusions are relevant to, but not exclusively for, stakeholder managers within the field of it-security.

Case

The case is based on best-practice advice given to consumers and citizens. The advice is formulated by stakeholder managers in the shape of it-experts, to help individual consumers and citizens to improve their own it-security. Within the specific case, the decision-makers did not follow the advice of stakeholder managers. This discrepancy is what allows for the case to fruitfully question theories of decision-making. The pieces of advice not followed by decision-makers are limited to five, but could have been different. The chosen number of advice allows the thesis to stay focused and clear, while still being able to deliver varying insights to the analysis of rationality in decision-making.

Research Design

The chosen approach was a case analysis. The case study was chosen to ensure that the analysis was relevant and contemporary. By introducing a case study the analysis and conclusions of the

thesis would be able to draw on relevant examples, thereby giving the thesis flesh to the bone. This way of using cases as a tool to improve the understanding is approved by Bent Flyvbjerg:

> "It is only because of experience with cases that one can at all move from being a beginner to being an expert. If people were exclusively trained in context-independent knowledge and rules, that is, the kind of knowledge that forms the basis of textbooks and computers, they would remain at the beginner's level in the learning process."[8]

This is especially relevant when the concepts of the thesis are concerned with relatively abstract phenomenons of decision-making, where the general rationality of the actor is questioned. The case study thereby improves the in-depth understanding of the theoretical analysis, but it does not, however, serve as proof of universality.

The case study on rationality in decision-making is assumed to be relevant outside the current field of it-security, with other links of decision-makers and stakeholder managers. Nonetheless, the case study does not statically give proof of such. Contrary, it is for further studies to prove that the conclusions of the thesis can be transferred to other areas of decision-making. However, as noted by Bent Flyvbjerg, this is not preventing analysis based on a case-study to have significant relevance:

> "The advantage of large samples is breadth, whereas their problem is one of depth. For the case-study, the situation is the reverse. Both approaches are necessary for a sound development of social science."[9]

To further highlight the relevancy of the findings within the analysis, conclusions and discussion, it would be needed to include further empirical data to prove the degree of universality of the findings. This could be done by increasing the number of case-study analyzes, or to insert the conclusions in experiments in order to do a test of validity.

[8] Five Misunderstandings About Case-study Research, Bent Flyvbjerg, Aalborg University, 2006, p. 222
[9] Five Misunderstandings About Case-study Research, Bent Flyvbjerg, Aalborg University, 2006, p. 241

Targeted reader

That stakeholder management is the onset of the thesis is due to objectively recognized issues of making consumers and citizens follow advice on the field of it-security. However, that groups or individuals are taking responsibility in a field, such as it-experts within the field of it-security, is not unique. Rather, it is seen within almost all sectors of human life that specific groups or individuals engage to change behavior of others. The management of decision-makers, who are stake holders within fluctuating fields, is what throughout the thesis is referred to as stakeholder management.

It is an underlying assumption of the thesis that the mechanics of decision-making is indifferent to the field. This means that decision-making theory, drawn from behavioral economics, can be introduced to different settings, still upholding a consistent degree of relevance. Therefore the recommendations and conclusions within the thesis, despite being based on a case analysis of it-security, are seen to be widely applicable. The fundamental expectations of the thesis is therefore that best-practice of stakeholder management is transferable to a broad section of stakeholder areas, whether this be consumers, citizens, athletes, smokers, house owners or tax payers.

Theoretical framework

Deductive approach

The thesis undertakes a hypothetic-deductive[10] approach. This means that the goal of the thesis is to come by theoretical conclusions, which later can be empirically tested if such a need arises. The purpose is thereby to explore the concepts of decision-making, with specific focus on the role of rationality. This assumption behind the research question that the understanding of rationality in decision-making is not at a state, where empirical hypothesizes can be formulated. The thesis is thereby centered on the ontological approach to an understanding of rationality, where it is not epistemologically questioned how the concept of rationality has been derived. Instead the thesis seeks to explain further the ontological concept of rationality, more specifically in connection to decision-making[11].

[10] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 27
[11] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 23

Definition of theory

The used definition of theory is one that lays weight to theory being explanations on patterns, which can be or is expected to be observed[12]. This definition is the foundation as to why the theoretical discussion within the thesis is important. By discussing the role of rationality in decision-making, by comparing opposing concepts, the thesis is able to present explanations on behavioral patterns. These explanations on behavioral patterns will not be empirically proven within the current dissertation. Instead, the thesis aims to open up the theoretical understanding, thus giving easier access as how further down the line conduct empirical studies. This results in the thesis living up to the criteria of academic inference, where it is demanded that science delivers new possibilities for further studies[13].

Chosen theory

In order to conduct such exploration of the role of rationality in decision-making, the theory of behavioral economics was chosen, because it is centered on analysis of human behavior. The choice of theory, stemming from behavioral economics, was done through selectively browsing through theories that would be able to open up the understanding of decision-making. The theories, who all take a stand on rationality in some manner, are not exhaustively explaining decision-making in all its perspectives. Besides this, a pedagogically harsh line between theory of rationality and non-rationality has been drawn. This was done for the purpose of giving a more clear understanding of rationality in decision-making, albeit losing a flow of flexibility in the analysis.

The theorists of rationality in decision-making are credited follow in the footsteps of Herbert Simon. Simon constructed the argument that decision-makers are perfectly rational, but rational within certain boundaries. The concept of rationality used, is therefore never one that at any point assumes perfect rationality. Gary Becker, Gerd Gigerenzer and Wolfgang Gaissmaier are contributing with angles and understandings that elaborate on bounded rationality.

The works of the different authors in collaboration is what constitutes the side of non-rationality. The lack of a binding author is making the combination of authors of non-rationality less intuitive.

[12] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 25
[13] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 105

However, the purpose is not to say which authors of non-rationality theory are describing decision-making with highest precision. Instead, the thesis is about discussing whether non-rationality theories of decision-making, as an entity, can be said to undermine the thoughts of Herbert Simon and likeminded theorists. The authors are representing concepts that are believed to be fundamental in non-rationality decision-making literature[14], however, this is also a point of deliberation.

Empirical data

Reports and articles

Collection of data

The case was based upon several reports on the field, all released recently to ensure case' relevancy. Of the authors behind the reports can be highlighted DKCERT, which is the Danish Computer Security Response Team, part of the National Research and Education Network in Denmark. DKCERT regularly release reports on the status of it-security in Denmark, focusing on the citizen's aspects of it-security in Denmark. For surveys on consumers, reports released by The Danish Consumer Council have been used. These two organizations are both concerned with the digitalization in Denmark, and are advocates of a strong focus on how this development pans out.

Beside these organizations, a wide range of articles have been included as case material. The validity of articles is always a case of concern, but the chosen sources have all been selected with quality in mind, furthermore, the articles are never the sole source of information, as reports conducted by respected institutions are the backbone of empirical data throughout the case.

Limitations of collected data

It is a fundamental assumption that the research behind the empirical data, taken from external sources, has passed criteria for free, independent and unbiased science. However, seeing as the case is simply used as a representative of decision-making in general, it is not the validity of the case that is in focus. Rather, the focus is whether the case is able to give examples of the role of rationality in decision-making. In principle, the used case could be purely theoretical, seeing as it is not the purpose of the thesis to definitively give answers on how to improve it-security among

[14] An Introduction to Behavioral Economics, Alain Samson, PhD, 2014.
Available at: https://www.behavioraleconomics.com/introduction-to-be/

consumers and citizens. Contrary, the thesis aims to deliver theoretical insights on rationality in decision-making, thus making the validity of theoretical conclusions unattached to the specific case of it-security.

Interviews

Interview of experts

To support the case, two interviews of experts on it-security were done. The first interview was of Peter Kruize, who is a lecture at University of Copenhagen, Faculty of Law. The second was of Christian Wernberg-Touborg, who is a board member of The Council of Digital Security, and also Chairman of the security committee at IT-Branchen. The interviews were done in person at two different time and locations in Denmark. Each interview lasted around an hour, and was recorded. The interviews have not been transcribed. The interviews were done in Danish, and have later been partially translated to English.

Choosing of experts

The two experts interviewed were selected, because they have are seen as protagonist of it-security. Peter Kruize has conducted several in-depth studies on digital fraud, especially with focus on identity theft[15]. This is why an interview of Peter Kruize was seen to give the report increased validity and reliability. Furthermore, an interview of Christian Wernberg-Touborg was done, because he has been quoted in several news articles on how it-security lacked attention, both in the public and by politicians. Christian Wernberg-Touborg was thereby relevant due to his opinions on the relationship between stakeholders and stakeholder managers.

Interview method

The interview was done by using a semi-structured interview model[16], see interview guide in the appendix. This semi-structured interview was chosen to allow for the needed knowledge to be obtained, still allowing flexibility to give room for new insights and perspectives. The interviews were done because specific empirical data more competently visualize the role of rationality in decision-making. Due to the fact that the interviewed persons were experts on their field, the interviews were both within the category of elite-interviews. This inevitably raised the level of required knowledge on behalf of the interviewer. Without such knowledge, the interview have a

[15] Kriminalitet i en digitaliseret verden, Peter Kruize, Faculty of Law, October 2013
[16] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 149

chance of being unbalanced, allowing the expert to dominate the setting[17]. Work-experience within it-security of the interviewer ensured that the needed knowledge was present.

From the interviews a dozen quotes have been used in the analysis and conclusion, this is done to achieve 'thick descriptions'[18]. This supply the reader with a richer context for improved envisaging. Qualitative interviews are compromised by the fact that the interviewer will always be active in the collection of data[19]. However, the qualitative interview was still favorable to gain access to 'thick descriptions'.

Method for analysis

The starting point of the analysis is the five pieces of advice given to consumers and citizens to boost their own it-security. Each advice is accordingly analyzed. First, the advice is analyzed by the concepts of bounded rationality, satisficing and ecological rationality. As the advice differentiates the case is able to shed different light on to which degree the concepts of decision-making with rationality finds merit.

Hereafter, the concepts of non-rational decision-making are put to the test. Because of the limitations of the time and length of the thesis, all six concepts of non-rationality have not been selected for each advice. Rather, concepts have been chosen as the representatives of non-rationality. The selection of non-rationality concepts, used to analyze each advice, was done to attain the highest degree of reliability and relevance to the theory.

Finally, the case analysis of every advice will be concluded by a confrontation of the theories of rational and non-rational decision-making. Thereby the arguments of rational and non-rational decision-making are examined, forcing the concepts to be confronted with a critique of the underlying assumptions.

Following the analysis is a conclusion, seeking to combine the theoretical findings of the case analysis. Concluding the thesis is given a broader perspective by recommending how to best

[17] Introduktion til et håndværk, Steinar Kvale and Svend Brinkmann, Hans Reitsels Forlag, 2008, p. 167

[18] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 146

[19] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 150

configure initiatives by relevant stakeholder managers with conclusions on the role rationality in mind.

Method discussion

Reliability

To answer the theoretically bounded research question, it was chosen to include a case analysis. This deductive method, by introducing empirical data to support a theory, was chosen because the research question concentrated on an ontological questioning of rationality. Seeing as the analysis was not inductive, using empirical data to formulate theory, the reliability is limited theoretical findings.

The conclusions are thought to be relevant when applied on other areas of empirical data, but has yet to be done. To improve reliability[20], a logical next step would be to continue deductively doing case analyzes that could showcase that the conclusions of the thesis can be repeated with different empirical data. Furthermore, the reliability of the case analysis could have been increased by performing additional interviews of experts, ensuring elimination outliers. This is why the interviews are only used as an additional secondary source of empirical data. The qualitative and quantitative reports are forming the baseline of the case.

Validity

That the case of it-security can accurately exam theories of decision-making is backed by several reports and studies concerned with discussing the decision-making of consumers and citizens in the field of it-security. Decision-makers (consumers and citizens) are acting against the advice of the stakeholder managers (it-experts). This underlines the strong connection between the chosen case and the theories of decision-making.

To increase validity, the thesis has also been concentrated on the defined question of rationality in decision-making. This excludes the ability to say that overconfidence or cognitive dissonance is non-existent, keeping the conclusions only defining the role of rationality within the theoretical concepts of decision-making.

[20] Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 101

With fewer concepts of rational and non-rational decision-making, the conclusions validity could have been higher, but by paying the prize of less universality. The reasoning to this is that the fewer concepts analyzed, less could be concluded on rationality, seeing as a smaller segment of behavioral economics theory would be represented.

Theory

Introduction to behavioral economics

Behavioral economics is in its core a way of opening up the otherwise closed of area of human decision-making[21]. Up to this, decision-making has been noted as being something purely connected to perfect information and a rational choice based upon this. However, in behavioral economics, the playing field becomes muddy as theories of non-rationality decision-making are contributed.

The concepts of non-rational decision-making are not only in opposition to the believers of perfect rationality. Even within the field of behavioral economics, there is a varying focus on the role of rationality within decision-making. The theories of Herbert Simon on satisficing are credited as among the cornerstones of behavioral economics[22]. Herbert Simon, Gary Becker, Gerd Gigerenzer and Wolfgang Gaissmaier are advocates of bounded rationality, imperfect information, ecological rationality and satisficing. These concepts will in the analysis function as the representatives of rationality in decision-making.

As representatives of non-rational decision-making is a combination of authors, who all come together on a notion of decision-making being done on a basis of non-rational tendencies. Six concepts of non-rational decision-making will be described as counterarguments to the concepts of bounded rationality. These six concepts are: mental accounting, overconfidence, prospect theory, cognitive dissonance, emotions and choice architecture.

The review of the theorists is done to set up the framework for an analysis of whether or not decision-making is bounded rational or non-rational. To visualize this, the analysis will draw on the case of it-security to exam the theories. The discrepancy between the digital threats and protective measures taken, serve as the token of envisaging the discussion between the two platforms of behavioral economics' theory.

[21] An Introduction to Behavioral Economics, Alain Samson, PhD, 2014.
Available at: https://www.behavioraleconomics.com/introduction-to-be/
[22] An Introduction to Behavioral Economics, Alain Samson, PhD, 2014.
Available at: https://www.behavioraleconomics.com/introduction-to-be/

Theories of rational decision-making

Bounded rationality

In 1978 Herbert Simon won the Nobel Prize on his works of bounded rationality. In his Nobel Lecture, Simon focused on the historical struggle between theories of perfect and bounded rationality. Simon throughout his paper is an advocate for bounded rationality, focusing on how the classical economic theory, with its assumption of perfect rationality, is supported neither theoretically nor empirically:

> "I believe it is the case that specific phenomena requiring a theory of utility or profit maximization for their explanation rather than a theory of bounded rationality simply have not been observed in aggregate data. In fact … it is the classical, rather than the behavioral form of the theory that faces real difficulties in handling some of the empirical observations."[23]

Instead, Simon is asking what proof there is to be found of perfect rationality and profit maximization. Contrary, Simon argues that when looking at empirical observations, the theory of bounded rationality is what finds relevance.

Gary Becker, as Herbert Simon, won the Nobel Prize, and therefore held a Nobel lecture. In his lecture, despite being a believer in rational choice, Becker descripted the limitations to decision-making. This description is one that quite clearly defines bounded rationality:

> "Actions are constrained by income, time, imperfect memory and calculating capacities, and other limited resources, and also by the opportunities available in the economy and elsewhere."[24]

This description of bounded rationality outlines how the ability to rationally make decisions is constrained by the income, time, memory and calculating capacities available. Summarized, it can be said that Herbert Simon and Gary Becker, with their definition of bounded rationality, accepts that decision-makers make choices based on imperfect information. However, seeing as perfect

[23] Rational Decision-making in Business Organizations, Herbert Simon, Nobel Prize Lecture, Carnegie-Mellon University, 1978, p. 349

[24] The Economic Way of Looking at Behavior, Gary Becker, Nobel Prize Lecture, University of Chicago and Hoover Institution, 1992, p. 386

information is an imagination, making decisions despite of this is not going against the principles of rationality in decision-making.

Satisficing

With this baseline as the general understanding of bounded rationality in decision-making, the concept of Satisficing can be introduced. Satisficing, as invented by Herbert Simon, is a contraction of the two words sufficing and satisfactory. By combining the words Simon tries to symbolize under what circumstances the actors make the decision among alternatives. With satisficing Simon introduces the thought of actors making a choice lingering on the balance of being "good enough". According to Simon it is important to include the concept of satisficing when noticing the basis upon which decisions are made. The reason behind this is that even though decisions are done on a basis of rationality, according to Simon, the rational choice can be something that is not necessarily optimal in the world of perfect information, but might be so in the empirically proven world of bounded rationality. Here Simon uses the degree of aspiration as the marker of when the self-invoked level of satisficing is met to the decision-maker:

> "As an alternative, one could postulate that the decision maker had formed some *aspiration* as to how good an alternative he should find. As soon as he discovered an alternative for choice meeting his level of aspiration, he would terminate the search and choose that alternative. I called this mode of selection *satisficing."*[25]

In a situation with restricted income, time, memory and calculating capabilities, the rational choice would be to perform an act of satisficing. The choice might not be optimal, but considering the fact that rationality will always be bound, the act of conducting satisficing is the most rational approach to decision-making. This makes suboptimal optimal, proving to Herbert Simon and Gary Becker that rationality maintains the key role in decision-making.

Ecological rationality

In newer literature, Gerd Gigerenzer and Wolfgang Gaissmaier in 2011 wrote their paper: Heuristic Decision Making. The two theorists are readers of Herbert Simon, and have based their work

[25] Rational Decision-making in Business Organizations, Herbert Simon, Nobel Prize Lecture, Carnegie-Mellon University, 1978, p. 356

largely on the ideas of satisficing and bounded rationality[26]. Gigerenzer and Gaissmaier explain how bounded rationality results in decisions being based on heuristics, more commonly known as rule of thumb. These heuristics, however, do not result in poorer decision-making. Decisions based on heuristics are on the other hand often more frugal, even with scenarios of less information giving better results:

> "A heuristic is a strategy that ignores part of the information, with the goal of making decisions more quickly, frugally, and/or accurately than more complex methods."[27]

Gigerenzer and Gaissmaier therefore not only accept the premise of bounded rationality, but builds on to say that bounded rationality can be a positive vector in decision-making. In their view, the decisions based on heuristics and bounded rationality is in fact often less-is-more. One of the main reasons for this is what is called ecological rationality.

Ecological rationality is centered on the fact that rational decision-making depends on the environment in which the actor makes the decisions. In an environment with a high degree of uncertainty, trying to calculate the exact outcome is often resulting in deprived decision-making. On the other hand, according to Gigerenzer and Gaissmaier, a simple heuristic rule, where parts of the information are not counted in, can generate better answers depending on the ecological rationality:

> "The study of ecological rationality results in comparative statements of the kind "strategy X is more accurate (frugal, fast) than Y in environment E or in quantitative relations between the performance of strategy X when the structure of an environment changes."[28]

In their paper, Gigerenzer and Gaissmaier use the example of a ball thrown. To catch the ball, one can either try to weigh in all factors: speed, wind, angle, temperature etc. Combined, this calculation would give a valid proclamation of where the ball would land. Contrary, the heuristic

[26] Heuristic Decision Making, Gerd Gigerenzer & Wolfgang Gaissmaier, Annual Review of Psychology, Max Planck Institute for Human Development, 2011, p. 452
[27] Heuristic Decision Making, Gerd Gigerenzer & Wolfgang Gaissmaier, Annual Review of Psychology, Max Planck Institute for Human Development, 2011, p. 454
[28] Heuristic Decision Making, Gerd Gigerenzer & Wolfgang Gaissmaier, Annual Review of Psychology, Max Planck Institute for Human Development, 2011, p. 457

'gaze', where the catcher simply fixates on the ball, could be an easier and more precise approach. According to Gigerenzer and Gaissmaier, the amount of uncertainty within the calculations makes the computational forecast unattractive, whereas the simple fixation of the eyes on the ball has fewer channels for error. This is because the ecological rationality does not support complicated equations compared to simple shortcuts. Gigerenzer and Gaissmaier thus argue that decision-makers relying on heuristics have been falsely judged as being stupidity or laziness.

Theories of non-rational decision-making

Mental accounting

The concept of mental accounting is, in short, when decision-makers make calculations that fit them the best, rather on actual math. This means that instead of relying on objective facts, the decision-maker do calculations that gives the wanted result. This sort of relativity with calculations, where the decision-maker shows flexibility in the evaluation of the situation, is what Eldar Shafir and Richard H. Thaler describes in their studies on the phenomenon of mental accounting:

> "Our purpose in this article is to understand some of the mental accounting rules that allow people the flexibility to value things in multiple, fluid, and inconsistent ways while still providing a modicum of discipline and authenticity."[29]

Shafir and Thaler thereby studies the behavior that allows value to "multiple, fluid and inconsistent"[30]. Shafir and Thaler exemplifies this through the consumption of wine.

Shafir and Thaler in their studies outline how the valuation of a bottle of wine depends on how the outcome of the wine is. If the wine is dropped on the floor, even a wine bought many years ago, the loss is taken as the monetary price of the wine when acquired. On the other hand, the respondents in the studies conceive an old, forgotten wine from the back of cabinet, consumed on the dinner table, as free. Objectively, the value does not fluctuate according to whether the wine is dropped on the floor or consumed, but participants in the study suggest that they think otherwise. Shafir and Thaler summarizes this as being irrational thinking, but as they put it:

[29] Invest now, drink later, spend never: On the mental accounting of delayed consumption, Eldar Shafir and Richard H. Thaler, Journal of Economic Psychology, Princeton University, 2006, p. 696
[30] Invest now, drink later, spend never: On the mental accounting of delayed consumption, Eldar Shafir and Richard H. Thaler, Journal of Economic Psychology, Princeton University, 2006, p. 696

> "Rational is not necessarily happy, and irrational gives you the rare opportunity to enjoy ''free'' drinks."[31]

The mental accounting of decision-makers is not rational, because personal preferences influencing the calculations cannot be objectively supported. Rather, the influencing of personal preferences, changing the outcome of the calculations on how to behave, distorts the rationality of the decision-maker.

Overconfidence

The phenomenon of overconfidence is not solely to be allocated to behavioral economics. However, within behavioral economics, overconfidence is widely accredited as being a factor in decision-making. In the works of Gokul Bhandari and Richard Deaves they look at exactly the phenomenon of overconfidence. Bhandari and Deaves display how overconfidence is somewhat a normal feature of human beings, albeit been represented increasingly in specific groups.

In their introduction they refer to the studies done on the better-than-average effect. Here numerous studies are showing that participants assume themselves to be better than average, and that this is thought so by more than 50 % of respondents:

> "In research setting, overconfidence can be detected and even measured in several ways. Some studies have asked people to rate themselves relative to average on certain positive personal attributes such as athletic skill or driving ablity. Genereally more than 50 % say they are better than average."[32]

Besides the considering themselves as better than the average, the self-attribution bias also contributes to overconfidence of decision-makers. These decision-makers are neglecting the faults when performed unsatisfying, such as betting against the market, but are taking credit when positive outcomes occur. This exemplifies a bias towards maintaining self-confidence even when facing defeat. According to Bhandari and Deaves, the overwhelming statistics showing

[31] Invest now, drink later, spend never: On the mental accounting of delayed consumption, Eldar Shafir and Richard H. Thaler, Journal of Economic Psychology, Princeton University, 2006, p. 696
[32] The demographics of Overconfidence, Gokul Bhandari and Richard Deaves, The journal of Behavioral Finance, The Institute of Behavioral Finance, 2006, p. 5

overconfidence is not rationally sound, as overconfidence leads to suboptimal results[33]. Furthermore, studies show how "market experience exacerbates overconfidence, primarily through knowledge deterioration"[34]. Here Deaves, along with Erik Lüders and Michael Schröder, describes how experience, despite of an increase in accumulated information, actually contributes to the deterioration of the ability to make rational decisions, which are based on objective knowledge rather than overconfidence.

Prospect theory

This theory is authored by Daniel Kahneman and Amos Tversky. Kahneman and Tversky presented prospect theory as a response to expected utility. In expected utility the decision-making is done on the basis on a neutral and logical assessment of outcomes. In expected utility it does not matter whether the decision is about losses or gains, because the outcome is always based upon a rational decision of the expected utility. Kahneman and Tversky sought to give a more relevant theory that correlated with empirical data:

> "In expected utility theory, the utilities of outcomes are weighted by their probabilities. The present section describes a series of choice problems in which people's preferences systematically violate this principle."[35]

To explain the lack of rationality in decision-making, Kahneman and Tversky presented 'loss-aversion'. Kahneman and Tversky introduced how loss-aversion affected decision-making in outcomes where the decision-makers were faced with losses and gains:

> "First, note that the reflection effect implies that risk aversion in the positive domain is accompanied by risk seeking in the negative domain."[36]

Loss-aversion made decision-makers risk-seeking when it came to losses, because decision-makers were willing to gamble in order to avoid losses. Therefore decision-makers were willing to toss a

[33] The demographics of Overconfidence, Gokul Bhandari and Richard Deaves, The journal of Behavioral Finance, The Institute of Behavioral Finance, 2006, p. 5
[34] The Dynamics of Overconfidence: Evidence from Stock Market Forecasters, Richard Deaves, Erik Lüders and Michael Schröder, Journal of Economic Behavior & Organization, 2010, p. 1
[35] Prospect Theory: An analysis of Decision under Risk, Daniel Kahneman and Amos Tversky, The Economic Society, 1979, p. 265
[36] Prospect Theory: An analysis of Decision under Risk, Daniel Kahneman and Amos Tversky, The Economic Society, 1979, p. 268

coin, when the scenario was to either loss a hundred dollars by not gambling, or by heads or tails to either owe five hundred, or break even. The decision-makers would rather take the chance to be debt free, neglecting the statistical chance of owing five times as much. On the other hand, when there is a gain involved, the participants were much less willing to stake it in order to either double the income, despite the statistical upside of doing the coin toss.

Besides loss-aversion affecting decision-makers, 'certainty effects' also proved to make participants less likely to gamble the more uncertain, despite favorable statistics. As Kahneman and Tversky puts it:

> We first show that people overweight outcomes that are considered certain, relative to outcomes which are merely probable – a phenomenon which we label certainty effect."[37]

The certainty of the outcomes changes the decision weights of the deliberation. This is shown by Kahneman and Tversky when looking at the rationality behind ensuring that there is no bullet in the gun when playing Russian roulette:

> "Would you pay as much to reduce the number of bullets from four to three as you would to reduce the number of bullets from one to zero? Most people feel that they would be willing to pay much more for a reduction of the probability of death from 1/6 to 0/6 than for a reduction from 4/6 to 3/6. Economic considerations would lead one to pay more in the latter case, where the value of money is presumably reduced by the considerable probability that one will not live to enjoy it.[38]

This combination of loss-aversion and certainty effects affecting decision weights is the backbone of prospect theory. By having relative decision weights, decision-makers do not follow the objectively most rational decision-model, in fact, they often seek risk when no risk is to be sought, and takes sure winnings when gambling is the soundest thing to do.

[37] Prospect Theory: An analysis of Decision under Risk, Daniel Kahneman and Amos Tversky, The Economic Society, 1979, p. 265
[38] Prospect Theory: An analysis of Decision under Risk, Daniel Kahneman and Amos Tversky, The Economic Society, 1979, p. 283

Cognitive dissonance

Matthew Rabin has done work on the psychological concept of cognitive dissonance. As a phenomenon, cognitive dissonance occurs when decision-makers are making decisions that are immoral according to their own standards, thus creating a gap between the correct behavior and the actual behavior. This might happen if the cost of not making the specific decision is heavy and the alternatives few. In such scenarios, cognitive dissonance allows immoral behavior to become tolerable. This diminishes the bad conscience, and allows for immoral behavior to be accepted:

> "Because it is unpleasant, people prefer to reduce cognitive dissonance. There are two ways to do so. As economists generally assume, people can change their behavior. Or - much less familiar to an economist - people can change their beliefs."[39]

For example, if the profits of investing in guns are supreme compared to other stocks, the investor might feel torn between the moralities of the matter. To justify investing, the investor convinces him or herself that it is the person pulling the trigger who is to blame for the murder. Furthermore, the investor can try to persuade others to follow his example, as to even further justify his own immoral actions by making them socially accepted. The survival technique of adjusting moral standards to fit the situation is what Rabin describes, when he argues against pushing people too much:

> "My main conclusion is that increasing the propensity of people to feel bad when they engage in immoral activities might actually increase the level of these immoral activities. This perverse effect could not occur with an isolated individual, but rather occurs only when members of society learn about and care about each other's beliefs about morality."[40]

By going too hard against the moral beliefs, pushing or forcing people to acknowledge their own immoral tendencies, might result in the opposite of correction. The push against people's bad

[39] Cognitive Dissonance and Social Change, Matthew Rabin, Journal of Economic Behavior and Organization, University of California at Berkeley, 1992, p. 178
[40] Cognitive Dissonance and Social Change, Matthew Rabin, Journal of Economic Behavior and Organization, University of California at Berkeley, 1992, p. 178

confidence might be followed by a turn to the worse, when the immoral behavior once done against better judgment, is now becoming the new standard.

Emotions

As another important author of theory within behavioral economics is Jon Elster, who has written about emotions. The emotions in decision-making are not something that traditional rational-choice models include, and according to Elster, this is a faulty absence. With emotions in decision-making, Elster adds to the table how feelings are affecting the way decisions are made. According to Elster, emotions need to be included into the tool kit of economics[41].

Rendering to Elster, emotions affect the way decisions are shaped, thus proving to be a duality of both shaping decisions as well as rewards:

> "The role emotions cannot be reduced to that of sharpening the reward parameters for rational choice. It seems very likely that they also affect the ability to make rational choices within those parameters."[42]

Elster argues that emotions are to be taken seriously when looking at decision-making. He puts forward the argument that emotions shape the framework around decision-making. In a case of a debate, emotions of the participants will thus affect the outcome. This is because feelings such as honor or pride influences how the participants decide to debate[43]. The influence of emotions on decision-making is exactly what Elster wishes to contribute with to the field of knowledge on decision-making:

> "How can emotions help us explain behavior for which good explanations seem to be lacking? This is the main focus of the present article."[44]

[41] Emotions and Economic Theory, Jon Elster, Journal of Economic Literature, American Economic Association, 1998, p. 47
[42] Emotions and Economic Theory, Jon Elster, Journal of Economic Literature, American Economic Association, 1998, p. 73
[43] Emotions and Economic Theory, Jon Elster, Journal of Economic Literature, American Economic Association, 1998, p. 47
[44] Emotions and Economic Theory, Jon Elster, Journal of Economic Literature, American Economic Association, 1998, p. 48

Thus the rational-choice model misses out on the influence of emotions, and cannot explain why a decision that according to objective rationality is the prevalent option, might not be the chosen way to go.

Choice architecture

The underlying assumption within choice architecture is that decision-makers will choose the most convenient option. There might be better alternatives; the decision-maker will choose the scenario involving the least degree of attention, consideration and efforts. This is why the default option is so often chosen. Richard M. Thaler, Cass R. Sunstein and John P. Balz authored a paper on the choice architecture of decisions-making. Within it, the authors elaborate how the fundamental reasoning behind decision-making is to prioritize convenience:

> "For reasons of laziness, fear and distraction, many people will take whatever option requires the least effort, or the path of least resistance. All these forces imply that if, for a given choice, there is a default option – an option that will obtain if the chooser does nothing – then we can expect a large number of people to end up with that option."[45]

Thaler, Sunstein and Balz thereby argue that even though the calculus of rationality could argue for any other option, the likelihood of the decision-maker to go with the convenient choice is overshadowing.

This means that the chances of decision-makers making the right choice do not rely on the reasoning of the individual. According to Thaler, Sunstein and Balz, thereby the rationality of 'plain old humans' is lacking when it comes to making the right decision among choices:

> "Economic agents are assumed to reason brilliantly, catalogue huge amounts of information that they can access instantly from their memories, and exercise extraordinary will power … Plain old humans make plenty of mistakes (even when

[45] Choice Architecture, Richard M. Thaler, Cass R. Sunstein and John P. Balz, Department of Political Science, University of Chicago, 2010, p. 4

> they are consciously thinking!) and suffer all types of breakdowns in planning, self-control"[46]

In other words, 'plain old humans' cannot be trusted to make conscious decisions that are rational. On the contrary, human decision-makers are more often than not faulty in their decision-making, selecting not the best option, but the convenient one.

[46] Choice Architecture, Richard M. Thaler, Cass R. Sunstein and John P. Balz, Department of Political Science, University of Chicago, 2010, p. 4

Case: It-security

Confidence among consumers and citizens

In 2017 the Danish Consumer Council released a study on the consumers' digital trust and feeling of safety online. The report, called Digital Security – The biggest challenges for the Danish consumers, focused on the current state of mind among consumers. Pointing towards the most recurring themes the report interviewed a representative number of consumers on their thoughts, behavioral patterns and fears when using the digital market.

When asked about the fears of using the digital features, the consumers and citizens in general display a great deal of self-esteem. As shown in the figure 3 below, a majority of 69% express a notion that they are able to navigate online in a safe and secure way. This is compared to only 19% expressing feelings of insecurity of navigating online. According to these numbers one could argue that the difficulties of consumers online are limited. However, when dipping deeper into the numbers, it becomes clear that the calmness of consumers do not follow when asked about specific situations.[47]

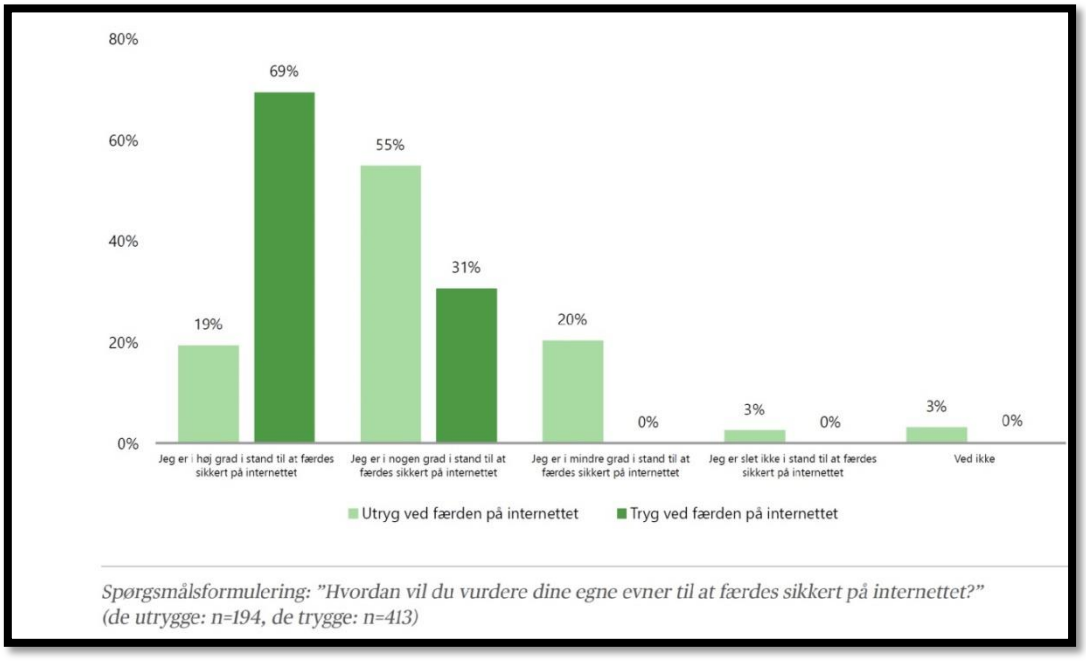

Figure 3: Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016, p. 54

[47] Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016, p. 54

When asked about the fear of having the credit cards misused 79% of consumers in the survey express concerns. When faced with personal identification numbers being abused a total of 74% convey that they are afraid of this happening to them. When it comes to misplacing of personal information by authorities, illegal distribution of personal information by companies, virus attained through e-mails, terms of use that are impossible to understand and unlawful tracking of data, a majority the consumers find themselves in a position of feeling uneasy at the thought[48].

This contradiction of data could be argued to be a display of the ambiguity consumers are feeling when using the digital and online opportunities. The digital sphere is offering many viable options of shopping, browsing and researching, but it also comes with a backlash of possible It-crimes. As described in the introduction this fear of It-fraud when asked about specific scenarios is not misplaced, as the numbers of digital fraud is on the rise, when almost all other kinds of crime is decreasing. The consumers therefore might be reluctant to the view of digitalization as something dangerous, yet when faced with actual events they more openly admit to having certain fears. In the following section of the study will be an account of the current state of It-security threats to consumers.

The risk of digital fraud

Following the increased attention on the field of it-security and it-crime, the amount of surveys on the field have increased. Looking on the financial side, researcher Peter Kruize has in the figure 4 below outlined that the outcome is within the millions of Danish Krones:

Tabel O.4 Samlet økonomiske tab

	Undersøgelse (kroner)	Estimat for DK (mio. kroner)
Identitetstyveri	311.127	59
Misbrug af betalingskortoplysninger	639.149	91
Bedrageri ved internethandel	779.489	81
I alt	**1.729.765**	**231**

Figure 4: Kriminalitet i en digitaliseret verden, Peter Kruize, Faculty of Law, October 2013, p. 6

Therefore the practical and financial consequences of being exposed to it-fraud is not only unpleasant, but also something that every year contributes to further funding of It-criminals.

[48] Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016, p. 52

Furthermore, according to surveys, it is only a fraction that is ever reported this to the police[49]. The reason might be connected to the nature of the crime, where the understanding is often that the police might be grasping for straws when chasing digital criminals:

> "The bulk of the incidents are not reported because the victims don't believe the police can do much about it, and then why have the trouble of reporting it […] This is partially because we see so many TV-shows and articles where the police are portrayed as not taking it seriously and not being able to do anything about it, and therefore I think that most victims simple accept the financial loss."[50]

This might explain the discrepancy between the reported incidents and the actual encounters of consumers with It-criminals. As the figure 5 below shows, the number of acclaimed incidents accumulated to 13% of consumers and citizens having been the victim of digital fraud:

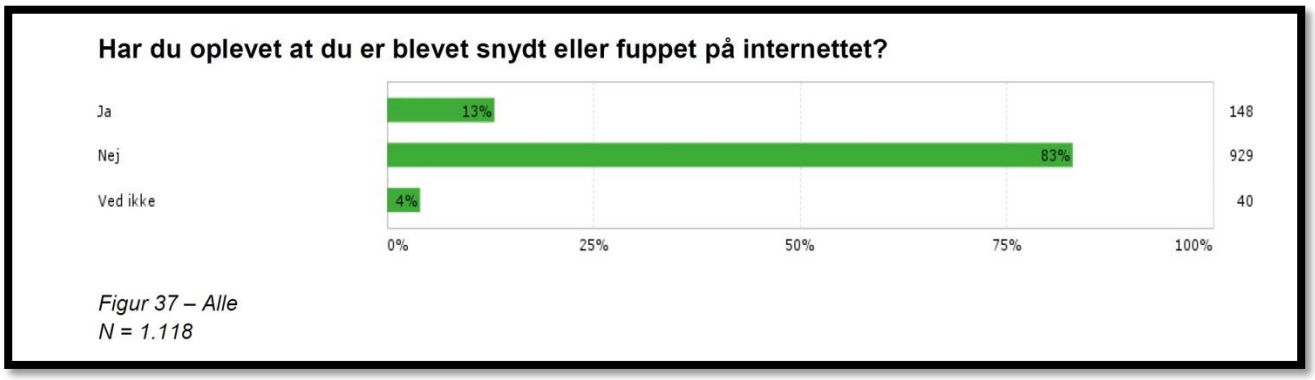

Figure 5: Online security survey, The Danish Consumer Council, March 2017, p. 27

Multiplying this to the quantity of consumers within Denmark, with a population of 5.6 million inhabitants, would mean that the reported cases of digital fraud should be at least half a million. Yet as outlined in the introduction, the skyrocketing accounts of digital fraud in 2016 "only" found itself at 22.339 cases.

It can therefore be hard to exactly outline the degree of which the Danish consumers are the target of digital fraud. Whether the rising number of reports is due to more and more people are

[49] Online security survey, The Danish Consumer Council, March 2017, p. 27
[50] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 26:30 min

starting to report their experiences[51], or if the growing number is a sign of an explosion of digital fraud, can be hard to define. The unknown number of not reported incidents of digital fraud mutters the picture, yet it seems to be clear that the future of digital fraud is big and seemingly on the rise. This means that the consumers in Denmark have every reason to introduce protective means. In the following paragraph the state of It-security among consumers will be explored.

Five pieces of advice

The best way to achieve digital protection does vary depending on who is given the question, yet some areas are most often described as necessary to achieve minimum standards of digital protection. The advice often includes installing software, doing maintenance, hesitancy and unique logins. Presented in the next part will be five of the most common advice on how to be protected from digital fraud[52].

Backups

Backup services are a way of taking a copy of all digital files, and storing them separately from the used device. By doing this the backups and be reintroduced in case the original device malfunctions, whether this is due to software or hardware complications. Many of these services are free, but with a cost when the needed storage exceeds certain limits. The concerned method of backups in the thesis will be those which are conducted through digital services. Among the most popular suppliers are Dropbox, OneDrive, Google Drive and iCloud. All of these services are continuously updated to give the users the most efficient experience.

Ransomware is an increasing way of conducting digital fraud, and it is one that is often successful to the criminal. In cases of ransomware it-criminals steal data, and only release the data after a ransom has been paid. Ransomware is nothing short of plain blackmailing, playing on the consumer's and citizen's vulnerability. Nevertheless, a recent backup will make the consumers and citizens much less vulnerable to this sort of blackmailing. Backups are useful in cases digital fraud and malware, preventing many consumers and citizens from being held ransom of it-criminals.

[51] Ofre for net-tyveri langer ud efter politiets jagt på digitale tyve, Danmarks Radio, Laura Marie Sørensen, October 2015.
Available at: https://www.dr.dk/nyheder/indland/ofre-net-tyveri-langer-ud-efter-politiets-jagt-paa-digitale-tyve
[52] 10 råd til sikker pc-brug, Digitaliseringsstyrelsen.
Available at: https://www.borger.dk/internet-og-sikkerhed/Sikker-selvbetjening/Se-10-gode-raad

Antivirus

Another frequently mentioned feature of digital protection is to install antivirus. Whether the name is Kaspersky Lab, F-secure, Norton or McCafee, these software programs all offer several services to stay protected online. The classic service is to scan the device for unwanted types of viruses, malware and spyware. Another feature offered by the antivirus is the firewall. Firewalls scan all incoming and outgoing data, searching for intended malicious content. By either warning the user, or by simply denying or removing unwanted segments, the firewall is the first line of defense for consumers and citizens. As shown in figure 6 below, recent tests of the most common antivirus software is showing a high degree of being able to detect the most widespread threats:

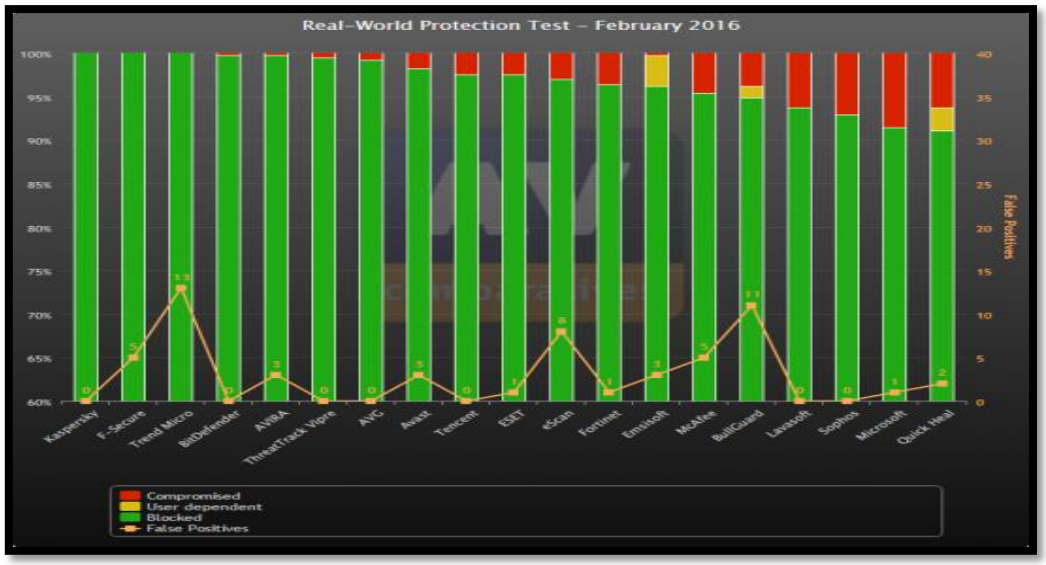

Figure 6: Stor sikkerhedstest: Her er det bedste antivirus-program lige nu, ComputerWorld, Nicolai Devantier, March 2016. Available at: https://www.computerworld.dk/art/236634/stor-sikkerhedstest-her-er-det-bedste-antivirus-program-lige-nu

The green is symbolizing the amount of malware being caught by antivirus. Some antivirus comes close to 100% efficiency, and as the test done by AV-Comparatives show, even the antiviruses with the lowest accuracy is catching more than 91.4% of all malicious software. Thereby even the software performing the worst is getting every 9 of 10 pieces of malware. So from the view of it-experts antivirus is something that is always recommended to install on PCs, smartphones and tablets.

Updating

Along with having backups and antivirus, most it-professionals refer to the growing importance of keeping updated on all devices. This is important for operating systems, Java, antivirus or media

players. By updating the software consumers and citizens can ensure that already known faults in the installed software is rectified. The software companies are in an ongoing search for faults and lacks in the programming code of their software, and will therefore ever so often release new patches to the software content. This improves the digital security of consumers and citizens by reducing the build-in flaws of the installed programs. Updating is especially crucial because software flaws are exposing the consumers and citizens without their notice. It is therefore in the hands of software companies to release software updates, but the responsibility of consumers and citizens to get them installed.

Skepticism

Another way of staying protected when being online is a more elusive one as such. As in other parts of life the slogan of something being "too good to be true", is also highly relevant in the realm of digital security. Few would not be tempted to get an almost free, very expensive, new iPhone. These offers, with examples shown in figure 7, often seem to origin from the most trustworthy of sources, yet it is the opposite being the case:

Figure 7: How to spot a 'Free iPhone' (or 'Free iPad') scam, Macworld, Lucy Hattersley, September 2015. Available at: http://www.macworld.co.uk/feature/iphone/free-iphone-ipad-scam-fake-auction-site-facebook-3608522/

Once the link within the E-mail, text or webpage has been clicked, it-criminals can take over the device of the consumers and citizens. This way of "phishing" careless consumers and citizens is no different than common scams in the physical world. Nevertheless, the consequences of buying a fake product often centers around the loss of a few thousand Crones, whereas in the digital world it is an entire digital life on the stake.

Compared to ransomware, where backups are efficient, there is no obvious solution to this conning of consumers and citizens, because it takes nothing more than a picture and some text to

send a phishing e-mail. Therefore the solution being broadcasted by it-experts is to display hesitation and a healthy skepticism. If consumers and citizens grew skeptic before giving away credit card information, a lot of misfortune could likely be prevented. A gut feeling of skepticism within the consumers and citizens is often what it-experts presents as among the most important thing keeping digital fraud from happening. This is why "if it seems too good to be true, it probably is", still works as a vital part of the consumers and citizens digital defense.

Passwords

Finally, there is no going around digital security without mentioning passwords. The ever increasing number of passwords having to be memorized is always a challenge. To gain access to the devices of the consumers and citizens, or to login into e-mail, Facebook, Twitter, bank or online newspapers, passwords function as an unavoidable part of the lives of consumers and citizens.

However, with passwords building up, the difficulty of keeping them all in tap becomes strained. The simple, and not advisable, solution among consumers and citizens is to write passwords down or to reuse passwords[53]. On top of this, many consumers and citizens connect their passwords to easily remembered phrases[54]. Whether the password is simply QWERTY or 123456, it does not take it-criminals more than a millisecond to guess. This easiness of cracking passwords becomes even more frightening when surveys suggest that around 50% of all passwords are among the top 25 most popular passwords[55]. In a hack of Dropbox in 2012[56], ironically a backup supplier, more than 65.000.000 accounts where hacked. With this sort of data spread out on the internet, it simple for it-criminals to login into several services, if the password and e-mail is the same.

Without unique passwords for every login, the consumers and citizens unwillingly disclose their digital life to it-criminals. Unique passwords ensure that the damage of a hack is contained, and that it-criminals cannot simply press 12345 to attain access to one's digital life.

---

[53] Reusing Passwords on Multiple Sites, Center for Internet Security, June 2016.
Available at: https://www.cisecurity.org/reusing-passwords-on-multiple-sites/
[54] Do you have one of the most common passwords?, The Telegraph, James Titcomb, March 2016.
Available at: http://www.telegraph.co.uk/technology/2016/01/26/most-common-passwords-revealed---and-theyre-ridiculously-easy-to/
[55] The Most Common Passwords of 2016, Keeper Security, 2016, p. 1
[56] Dropbox hack leads to leaking of 68m user passwords on the internet, The Guardian, Samuel Gibbs, August 2016.
Available at: https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

Advice not followed

However, when researching the status of degree of which the pieces of advice are being followed, the numbers do not look promising. In a study conducted by DKCERT in 2016, 61% of respondents do not on a regular basis secure a backup[57]. This is, as described, unfortunate when looking at how the backup of data can be a way to be protected especially against ransomware, which is a growing concern. In 2017 the ransomware attacks called WannaCry and NotPetya in is estimated to have been responsible of financial loses within the hundreds of billions of Danish Crones[58]. Furthermore, only 8% of consumers and citizens are not afraid to lose digital data[59].

When looking at the extent of consumers and citizens having an antivirus program installed the numbers is comparable to the figures of consumers using generic passwords. Only 50% have installed antivirus on their PCs[60] and 25% on smartphones and tablets[61]. This results in consumers and citizens not only endangering their own digital life, but also paves the way for it-criminals to spread digital fraud through infected devices. With such a low number of antiviruses installed on PCs, smartphones and tablets in Denmark, the consumers and citizens go against the advice of it-experts on how to lower the risk of digital fraud.

On the area of keeping the software updated there is also clear signs of not doing what can be done. This is most recently showcased with the international outbreak of the ransomware known as WannaCry. The WannaCry ransomware attack happened in May 2017, and was only able to happen because of system flaws in older versions of Windows installed worldwide. A lot of these PCs were even part of the critical infrastructure[62]. In surveys done on consumers and citizens, when asked about updating of antivirus, operating system and browser, around 30%[63] of participants admitted they had no general focus on updating these significant pieces of software.

[57] Trendrapport 2016, DKCERT - DEIC, different authors, 2016, p. 12
[58] Cyberangreb kan koste trecifret milliardbekøb, Fyens Stiftstidende, Ritzau, July 2017.
Available at: http://www.fyens.dk/erhverv/Cyberangreb-kan-koste-trecifret-milliardbeloeb/artikel/3167992
[59] Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016, p. 73
[60] Opråb efter hackerangreb: Husk nu at opdatere dit antivirusprogram, Danmarks Radio, Per Bang Thomsen, May 2017.
Available at: http://www.dr.dk/nyheder/indland/opraab-efter-hackerangreb-husk-nu-opdatere-dit-antivirusprogram
[61] Danskernes Informationssikkerhed, DKCERT, DEIC, different authors, 2017, p. 37
[62] UK hospitals hit with massive ransomware attack, The Verge, Russel Brandom, May 2017.
Available at: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin
[63] Online security survey, IDA, 2017, p. 2

The high number of consumers and citizens using outdated operating systems on their PCs, along with the third of consumers and citizens not paying attention to the need to update, exemplifies the gap between the advised guidelines to update, and then the reality among consumers and citizens.

When looking at the degree of consumers and citizens listening on the advice on having to be more hesitant before clicking on links, visiting webpages and answering phone calls, it is more challenging to get a clear view. Whereas surveys can be made on whether or not backups are being done, one cannot ask consumers and citizens if they act with the correct degree of hesitance in the digital sphere. Nonetheless, the growing accounts of digital fraud being reported shows a clear correlation between increased use of digital services and digital fraud. The curve of digital fraud is accelerating, and this an indicator that consumers and citizens are not invoking a healthy skepticism to take the necessary precautions in order to protect themselves.

Finally, over 50% of all passwords are among the top 25 most popularly used combinations. This is highly critical seeing as having unique passwords is among the first steps to take in order to take control of the ones digital security. Furthermore, in a survey conducted by DKCERT, it is described how 57% of the digital users have the same password for more than one service[64].

When looking at the development within digital fraud, and the personal and economic ramifications of such, one would assume that consumers and citizens would be paying more attention to the most recommended pieces of advice. Therefore it can be argued that consumers and citizens, not acting with protective initiatives in an unsecure situation, is making decision-making not involving rationality. However, it stands to be discussed whether the behavior of the decision-makers, here in the form of consumers and citizens, cannot be explained through rational argumentation.

In the following segment the case of it-security will be used to test, compare and exam the theories of rationality and non-rationality within decision-making. This constitutes the analysis of the thesis. The five pieces of advice will individually be used to analyze the theoretical concepts. Each part-analysis will be summarized by a short conclusion.

[64] Trendrapport 2016, DKCERT - DEIC, different authors, 2016, p. 12

Analysis: The role of rationality in decision-making

No backup and (no) rationality

The advice – do backups

The argument as of why to do backups has been shortly described in the previous sections. Here the main argument is that doing a back-up of one's digital life greatly enhances the resistance to ransomware and malware attacks. Backups are the main tool when looking at the chances of recovering hacked data that has been encrypted. The recovery of data through a back-up can make sure that it-criminals have less bargaining power in a blackmailing situation, where the key to unencrypt the locked data is sold via backchannels. Despite the benefits of doing backups, designated by it-experts, the advice is not followed by a majority of the population[65]. Citizens and consumers are thus not going along the advice that is seemingly the rational action to take.

Rationality - Bounded rationality

According to Simon and Becker the lack of backups might not be irrational, but rather bounded rational, or ecologically rational. Within certain conditions the rationality of the actions done by the decision-maker might be rational; despite being irrational within different settings. In the cause of backup's one angle to this could be that it is still a minority who has ever needed their backups, because widespread digitalization of documents and photos is still a relatively new phenomenon. Besides this the targeting of individual consumers and citizens by it-criminals is an even newer occurrence[66]. This might result in the understanding that backups are not worth the hassle. Thereby the knowledge available to the consumer and citizen is not that backups are unavoidable, rather backups are seen as a thing they are told to do, but never have needed. Without a need to occasionally revisit the backups for withdrawal of lost data, backups have to be considered as insurance. The newly emergence of the phenomenon of digital fraud against private consumers and citizens might prevent this being incorporated yet. The ecological rationality of the consumers and citizens is thus based on the fact that they have never needed their backups as insurance.

[65] Trendrapport 2016, DKCERT - DEIC, different authors, 2016, p. 12
[66] Private er i stigende grad mål for IT-kriminelle, Danmarks Radio, Mads Allingstrup, January 2015. Available at: https://www.dr.dk/nyheder/viden/tech/private-er-i-stigende-grad-maal-it-kriminelle

The clinch between the ecological rationality of consumers and citizens and the ecological rationality of the experts is also a growing issue within other fields. During recent years consumers and citizens have been told to follow rules on for instance food choices or physical exercise. This has resulted in consumers and citizens periodically being afraid of sugar, fat or eggs[67], only later to be replaced by new advice on sometimes completely contrary eating habits. With experts giving changing messages when it comes to best practice, it is within the ecological rationality of consumers and citizens to be somewhat skeptical to introduce initiatives that once again protects them from invincible threats. Consumers and citizens most likely rationalize that they are not willing to change behavior until the digital threat is concerned with them personally. As Peter Kruize puts it, the consumers and citizens wants to use the digital world despite of the "terms", and they do not change behavior until the point when they themselves are exposed, thus changing the ecological rationality:

> "If you have to read the terms when downloading an app, it will be too cumbersome, and if you then find yourself not willing to accept the terms, then what are you supposed to do? Therefore I think that most simply accept it the way it is, but of course this changes the moment you are exposed to digital crime. You change your behavior after that."[68]

A heuristic rule of thumb could also be to focus on the present and to accept losses. This is supported by how many major events in the lives of the decision-makers cannot be controlled. A loss of data thus might be unwanted, but faced with the impossibility of preventing all losses; it is a satisfice within the ecological rationality. The heuristics of not caring about backups is a way to cut through endless protective means against losses, relying on an acceptance of losses to make up for a lack of backups. The mindset being if it happens, it happens, nothing one can really do about it. This rationality, although maybe unwise on it-security, is beneficial when living in for instance tropical parts of the world, where flooding and hurricanes are part of life. And as Peter Kruize puts it, it is not because the consumers and citizens lack an understanding that there is a risk to be hit by hackers:

[67] Spis æg med god samvittighed, Søndagsavisen, Trine Fisker, May 2016.
Available at: https://www.sondagsavisen.dk/mad/madogsundhed/2016-03-23-spis-aeg-med-god-samvittighed/
[68] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 3:12 min

> "The vast majority have in on their mind that there is a concrete threat of digital fraud, and especially because they hear a lot about hacking, and that people can access the camera in your iPad, I think the majority are aware of the phenomenon of it-crime, and also sees it as a threat."[69]

Consumers and citizens can be argued to be skeptic to the prominence of backups, because within their ecological rationality, they have yet to witness the proof of backups being important. Besides this, there are reasons as to why heuristic rules of thumb to ensure an acceptance of losses being a part of the ecological rationality. Together it contributes to the idea that the lack of backups is rational within the bounded rationality, and is a result of satisficing between the restrained amounts of time, money, memory and mental capabilities[70].

Non-rationality - Prospect theory

Going against the portrayed rationality within not doing backups is the theory of prospect theory. In line with the theory, rationality is distorted by loss-aversion, explaining why consumers and citizens prioritize an avoidance of risk at any cost, contrary to a rational calculation of pros and cons. When it comes to the case of doing backups; it is a net expenditure to invest in a service from a provider of online storage, but also an expenditure when hit by digital fraud[71]. However, the consumer and citizen are only concerned with sure losses when they up-front purchase backups. Contrary it is only if the accident is to happen, and the consumer or citizen is successfully hit by digital fraud that there is a possible payment to it-criminals. But seeing as not every consumer has or will be the recipient of a hacker attempt, this cost is merely possible.

When paying for a backup service, or if paying for the key to unencrypt data, consumers and citizens, representing decision-makers in general, are forced to choose within decisions of loss. The differences being who receives the money, how much and at what point payment is due. Here it-criminals, in the eyes of the loss-averse, deliver a better service: You only pay when you are actually hit by an accident. This means that due to the nature of loss-aversion within prospect

[69] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 0.58 min
[70] The Economic Way of Looking at Behavior, Gary Becker, Nobel Prize Lecture, University of Chicago and Hoover Institution, 1992, p. 386
[71] WannaCry Ransomware Demonstrates The Value Of Better Security and Backups, Forbes, Tom Coughlin, May 2017. Available at: https://www.forbes.com/sites/tomcoughlin/2017/05/14/wannacry-ransomware-demonstrations-the-value-of-better-security-and-backups/#3d52085f70b8

theory, the consumer and citizen will be willing to engage in risk-seeking behavior in order to minimize the costs. In specific action this means that the consumer and citizen are willing to risk getting their data encrypted, compared to paying up front a cost, although smaller, that there is no chance to regain. In other words, the cost of paying for backups today is worse than having to only possibly pay it-criminals sometime in the future.

Non-rationality - Choice architecture

Besides loss-aversion, it is relevant to look upon choice architecture when discussing whether or not rationality is involved when consumers are skipping out on backups. The core idea of choice architecture is that actors, in this case the consumers and citizens, the representatives of decision-makers in general, would not be doing backups if it is not structured as the default setting.

To the likely frustration for it-experts this is not the case with backups, as there is not a backup function automatically in place for consumer or citizens. This lack of convenience is something that backup providers are aware of, and by creating recognized folders on the desktop, the backup providers have sought to close the gap between the wanted behavior and the default behavior. The instance that consumers have as a default setting that their documents and photos are stored within the synced folder, the change in behavior needed from consumers and citizens is redundant. Yet is poses as an issue that that before the correct choice architecture is nudging consumers and citizens to have the wanted behavioral patterns, there is a need to take an active stance on whether or not to engage with a backup provider.

To set up a backup solution that automatically saves copies of important data, the decision-making consumer and citizen, would need to take time aside for searching, downloading, installing and configuring the software. The whole process might take less than half an hour, but the matter persists when consumers and citizens will conduct the behavior posing the least amount of inconvenience. As Peter Kruize supports Thaler, Sunstein and Balz:

> "I think that as long as the individual can choose, one will choose the easy option, because the thought is that why make it harder than is has to be for oneself?"[72]

[72] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 8.53 min

By this statement Peter Kruize is supporting what Thaler, Sunstein and Balz argues when they state that the most important criterion defining decision-making is that the actor is first and foremost seeking convenience. Thereby the lack of backups, despite the accessibility, comes to prove that consumers and citizens, as decision-makers, do not engage in behavior that is inconvenient, no matter the benefits of going the extra mile. This lack of rationality in not doing backups is one that supports Thaler, Sunstein and Balz in their claim that decision-making is not founded purely on rationality.

Non-rationality - Mental accounting

Besides choice architecture theory and prospect theory, mental accounting contributes equally to weigh in on the side of non-rational decision-making behind the lack of backups. The mental accounting is clear when consumers and citizens, when asked about the fear of losing data, express concern in a degree, so it is only 8% not being afraid of losing data from digital fraud[73]. On the contrary it is less than half of the population that is doing backups, which is, as previously described, the most efficient tool to avoid loss of data.

The discrepancy between the awareness of a threat, and a hesitance of acting upon it, can most clearly be explained through mental accounting. As Shafir and Thaler describes it, the actual knowledge of a phenomenon does not prevent the decision-maker from changing mental accounting. This involves consumers and citizens putting up rules of thump resting rather on what is the wanted truth than the actual objective truth. This might involve saying that it is probably only if one visits certain sites that digital fraud can be experienced. Furthermore it could also be to calm oneself that the target groups are only men or women/young or old/rich or poor. By making up such exemptions the consumer and citizen can swap out the apparent risk with a more modest calculation, relieving oneself from the bad consciousness of not doing backups. This supports the previous section of choice architecture with a framework of even convincing oneself that convenient choice is the favorable choice.

The irrationality of the matter might be impractical in case an actual infringement of digital fraud on personal data occurs, but until then, the convenience acquired is satisfying to the decision-

[73] Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016, p. 73

maker. This is what Shafir and Thaler refers when giving mental accounting credit of being able to poor “free drinks”, but with a possibility of heavy hangovers the next day.

Bounded rationality or non-rational reasoning

According to Simon and Becker, the lack of backups would be a result of the ecological rationality at play. The limited information available, along with the limited cognitive capabilities, is thus the reason as to why the consumers and citizens avoid backups. This argumentation is supported by how the rationality of it-experts is not necessarily shared by consumers and citizens, who are not in possession of complete information on digital fraud and ransomware.

Furthermore, as a rule of thumb, it is explanatory that consumers and citizens obtain habits based on self-obtained experiences. The decision-making is thus to satisfice while relying on the information obtained and available, which is in this scenario creating a local ecological rationality where backups are not needed. Combining this ecological reality, where backups are redundant, with the fact that they cost money, time and energy, with a general skepticism to expert advice, the satisficing of consumers and citizens might rationally be to avoid doing backups, thus supporting Simon and Becker in stating that the individual is satisficing within bounded rationality.

However, when looking at the obvious benefits of doing backups in order to save data, admitted by consumers and citizens to be a major concern, the redundancy of backups decrease. This makes the viewpoint that not doing backups is an example of rationalizing behavior indecisive. Contrary, the theory of loss-aversion, convenience seeking and “Free drinks”, all gives answers as to why the decision-makers do not follow the seemingly rational option of doing backups.

Nevertheless, if the loss-aversion is making the decision-maker act against statistics, it could be argued that it is because, within the ecology at play, this is rational behavior. An underlying assumption within the ecological rationality could be that there will never be a point, where the decision-maker can duplicate everything of importance. This means that despite not doing backups is irrational in the field of it-security, having a realistic expectation of losses occurring is not. This most likely could result in loss-aversion, because even though losses are naturally happening, the act of diminishing losses can contribute to increased utility.

This ecological rationality of loss-aversion might not be one that can be justified consciously by the individual decision-maker, because the societal understanding of behavioral patterns has developed slowly and are intricate. However, by indulging in mental accounting and convenience seeking, the discrepancy between the ecological rationality and the rationality of it-experts is diminished.

To satisfice into not doing backups, when only 8%[74] argue that their digital protection of data suffices, is not a satisfying outcome from a point of perfect rationality. Yet, when comprising bounded rationality into the consideration, with ecological rationalities involving evolutionary traits to accept unexpected losses, along with locally gathered information being prioritized, the argument of rationality is dominating. Despite of this, loss-aversion, convenience seeking and flexible accounting are allowing the decision-makers to feel conveniently comfortable despite not doing backups, thus funding it-criminals through the payment of ransoms[75].

No Anti-Virus and (no) rationality

The advice – Install antivirus

When looking at the advice to install antivirus all PCs, smartphones and tablets, it is a piece of advice with a lot of the same features as the previous advice of doing backups. Just as with backup, antivirus is a matter of buying and installing a piece of software that will, according to experts, greatly increase the consumers' and citizens' digital protection. With around 9 out of 10 digital threats being caught by antivirus, it is a potent mean in the fight to stay protected[76]. This direct impact would assumingly make it attractive to consumers and citizens, and therefore it is a point of interest that only around 26 % of the Danish consumers and citizens have installed antivirus on their tablets and smartphones[77], and 50 % on their PCs[78].

[74] Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016, p. 55
[75] It-sikkerhed: Stigning I ransomware angreb er ude af kontrol, Version 2, Morten Egedal, February 2017. Available at: https://www.version2.dk/artikel/it-sikkerhed-stigning-ransomware-angreb-ude-kontrol-1073737
[76] Stor sikkerhedstest: Her er det bedste antivirus-program lige nu, ComputerWorld, Nicolai Devantier, March 2016. Available at: https://www.computerworld.dk/art/236634/stor-sikkerhedstest-her-er-det-bedste-antivirus-program-lige-nu
[77] Danskernes Informationssikkerhed, DKCERT, DEIC, different authors, 2017, p. 37
[78] Opråb efter hackerangreb: Husk nu at opdatere dit antivirusprogram, Danmarks Radio, Per Bang Thomsen, May 2017. Available at: http://www.dr.dk/nyheder/indland/opraab-efter-hackerangreb-husk-nu-opdatere-dit-antivirusprogram

Rationality - Bounded rationality

Despite the obvious benefits objectively outlined by it-experts, the ecological rationality of consumers and citizens might be otherwise. The reason being that digital protection through installation of antivirus is, with the limited information available, not only beneficial. With any sort of intricate software there is a price to be paid, and with antivirus the payment is due up front, like the "insurance" of conducting regular backups with a provider. This payment is, just as in the case with backup providers, as price that has to be paid no matter if the consumer and citizen are instigated by it-criminals.

Considering whether or not to invest in antivirus for their smartphones and tablets, the consumer and citizen is, according to Simon and Becker, not in a position of having perfect information and endless resources. Rather, the consumer and citizen are better off to follow a rule of thumb, as Gigerenzer and Gaissmaier describes it. With rule of thumb the decision-maker can sort off redundant information. The general statistics is thereby not as relevant compared how the neighbors, family and friends are doing decision-making. On a statistical level this might be insufficient, considering the vanishing chances of the immediate surroundings being statistically representative, yet on a basis of satisficing, it is adequate. Thus the relatively new emergence of digital fraud, resulting in fewer people having experienced the phenomenon, can be the underlying factor as to why consumers and citizens hesitate to install antivirus. Because if the heuristic is that: "I will do as my immediate surroundings", then the relatively new threat on private consumers and citizens[79] affect the understanding of antivirus being vital. As Christian Wernberg-Touborg describes it:

> "We have never witnessed that the digital infrastructure falls apart. This has a lot of consequences because we keep on building on the digital infrastructure, but without looking at the way the digital infrastructure is connected. The longer we wait the bigger the consequences will be one something happens, and something will eventually happen."[80]

[79] Private er i stigende grad mål for IT-kriminelle, Danmarks Radio, Mads Allingstrup, January 2015. Available at: https://www.dr.dk/nyheder/viden/tech/private-er-i-stigende-grad-maal-it-kriminelle

[80] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 7.04 min

As Wernberg-Touborg puts it, the digital infrastructure has yet to be broadly effected by digital criminals doing either malware attacks or digital fraud. Compared to flooding, hurricanes or power shortages, the common consumer and citizen have not yet had any experiences of a digital infrastructure hit by digital criminals.

Consumers and citizens following a heuristics of doing the same as the immediate surroundings might be rational from a satisficing point of view until the ecological illusion changes. The theory of ecological rationality is thus sustained by how a faulty reasoning can be self-sustaining the objectively irrational behavior. The ecological rationality will therefore only change once the local understandings among consumers and citizens change.

Another explanatory factor that supports Simon and Becker in their claim that all decision-makers satisfice within bounded rationality, is how antivirus slows down devices by up to 20 %[81]. With an imperfect understanding of the importance of having antivirus, the fact that the software even slows you down does not contribute to changing the ecological rationality. Just as wearing the seatbelt would be less appreciated if it would result in a car with 20 % diminished engine power. This contributes to why consumers and citizens, who already see their first rule of thumb not fulfilled, are inclined to skip the antivirus. This is especially supported by how PCs, smartphones and tablets are almost an extension of the body in the 21st century[82], making antivirus a self-induced stupifier.

A combination of not seeing the threat in the immediate surroundings, combined with the resistance to losing the computational edge, is what constitutes that consumers and citizens acting according to bounded rationality, satisficing and ecological rationality will not install antivirus.

Non-rationality - Prospect theory

Explaining the lack of antivirus from a non-rationality angle would be prospect theory. The fact that the costs of buying and installing antivirus, just as was the case with backups, is a certain cost, might be catalyzer for not engaging with antivirus. The benefits of antivirus are only real and

[81] Endurance Test: Does antivirus software slow down PCs?, AV-test, Markus Selinger, April 2015. Available at: https://www.av-test.org/en/news/news-single-view/endurance-test-does-antivirus-software-slow-down-pcs/

[82] The Extended Mind Thesis, Oxford Bibliographies, Julian Kiverstein, Mirko Farina and Andy Clark, October 2015. Available at: http://www.oxfordbibliographies.com/view/document/obo-9780195396577/obo-9780195396577-0099.xml

concrete the moment a real threat is prevented, and in those cases the consumer and citizen most likely will never be aware of the danger dodged. In other words, the benefits of antivirus are possible and invincible, whereas the immediate cost of buying and installing antivirus can be seen on the bank account right away. Whether consumers and citizens are paying antivirus providers or it-criminals the consideration is always about minimizing losses, not maximizing winnings. This means that when considering prospect theory, where the decision-maker is considered loss-aversive, the consumer and citizen might be more inclined to gamble with one's digital protection. By gambling with it-security of the PC, smartphone and tablets, the consumer and citizen give themselves the possibility of walking away with no losses at all, and with a mindset of loss-aversion, this is highly attractive. The discrepancy of consumers and citizens not using antivirus, albeit being effective and affordable, compared to the vulnerability and expensiveness of being exposed to it-criminals, supports the claims of Kahneman and Tversky when stating that decision-makers are making decisions on a foundation of loss-averseness.

Non-rationality - Choice architecture

The nature of decision-makers, such as it is portrayed within choice architecture theory, is that the convenient option will be the one chosen. For antivirus there has been a development within Microsoft Windows operating system that has changed the default option for consumers and citizens. Previous to the launch of Windows own antivirus program, Windows Defender, there was no antivirus default option within Windows. This meant that if the user did not actively protect them, they were completely unprotected by any sort of antivirus and firewall. After the release of Windows Defender in 2006 by Microsoft, there is now a default option including an antivirus program. In a survey done by DKCERT it is noted that 22 % of installed antivirus came preinstalled on the PC. This means that the availability of having an antivirus preinstalled has helped as much as 1 out of 4 with having antivirus, with the premise that consumers and citizens could have attained free antivirus otherwise if not for Windows Defender.

With a need for it-protection of convenience seeking consumers and citizens to be enhanced, the most promising way according to Thaler, Sunstein and Balz, is to introduce a default antivirus. The lack of a default antivirus on smartphones and tables is likely the reason why only 22% of these devices have antivirus. Therefore the dominant occurrence of antivirus on device with a convenient default option supports Thaler, Sunstein and Balz when arguing that the convenience

of the decision-maker is crucial. As Christian Wernberg-Touborg explains it, it is not only a lack of knowledge that results in consumers and citizens not installing antivirus on all their digital devices:

> "One explanation to the lack of It-security is a lack of knowledge, and the other is convenience, and convenience is a major part of this … The whole convenience of it being easy is extremely important compared to whether or not you are willing to use the product or not."[83]

Bounded rationality or non-rational reasoning

The theory of bounded rationality and satisficing is supported by the fact that the usage of antivirus has not yet achieved majority among consumers and citizens. This means that the way most decision-makers intuitively attain behavioral patterns does not encourage installation of antivirus. Furthermore, the importance of having fast and efficient devices, in a world where most spend hours every day being digital, clinch with the fact that antivirus slows down the computational speed. This combined makes for a strong case that the rationality of consumers and citizens is simply, within the imperfect information available, that the most rational behavior is to skip antivirus.

Going against this theory is the concept of choice architecture. Choice architecture is assuming lazy and convenience seeking decision-makers, and is backed by the fact that default antivirus on PC's has shown impressive results.

However, that default antivirus boosts installations can also point to decision-makers expecting it-security to be something someone else is in charge off. In the modern society, decision-makers usually choose among options that have all been deemed acceptable. This is often from legislators, who set up and test for minimum requirements. By such, it seems in a version of Gigerenzer's and Gaissmaier's ecological rationality, where decision-makers are used to default options being preapproved, would, although faulty, assume it-security on their devices to be handled.

Therefore it seems difficult to exclude that it is simply a lack of knowledge resulting in consumers and citizens not being aware that antivirus is needed. The prioritization of a smaller amount of

[83] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 49.40 min

money saved on antivirus now, instead of a possible bigger loss in the future when dealing with digital fraud, seems to support Kahneman and Tversky. Nonetheless, as with backups, it seems certain that consumers and citizens weigh in the local surroundings, where the phenomenon of digital fraud has yet to have dire consequences in the digital infrastructure. This might deconstruct that it is loss-aversion resulting in a lack of purchased antivirus, rather than simple frugal considerations. Thereby, the lack of antivirus among consumers and citizens is backing the rationality theory of Simon and Becker when saying that the behavior of decision-makers might not be completely rational, but it is rational within the ecological rationality at play.

No updating and (no) rationality

The advice – Update devices

Updates are crucial, as they are a way for software to be fixed. In it-security it is highly important to close gaps in the coding, not allowing for unwanted access of it-criminals. The updates are often released, and the more important and fundamental the piece of software is, the more endangering it is not to be updated regularly. Therefore it is among the most crucial segments of it-protection that consumers and citizens continuously update their PCs, smartphones and tablets.

The degree of consumers and citizens staying updated, however, leaves room for improvement. In a survey done by the union of engineers in Denmark, IDA, around 30 % only occasionally made sure that their devices were updated[84]. This means that in 1 out of 3 devices the consumers and citizens have are potential victims of it-criminals. Thereby the consumers and citizens do not only risk losing their own personal data, but they are also jeopardizing the spread of viruses, malware and spamming to others.

Rationality- Bounded rationality

With backups and antivirus it was reasoned that there could be found several heuristics resulting in a lack of following the advice. Especially the influence by surroundings might sway consumers and citizens to satisfice with a lack of backup and antivirus. Where backups and antivirus share characteristics, there is another setup for updating of software. Updates are not a new piece of software, but rather about improving the already installed software. Furthermore, updates differ in that it is without any costs to it. Updating software such as Java, Adobe or Internet Explorer is

[84] Online security survey, IDA, 2017, p. 2

almost always free of charge, and is seen by the companies as a must in order to deliver a competitive product on the market.

While the drawbacks are limited, the benefits of installing updates is overwhelming; the updating of software often improves the performance of the device, where slow coding is replaced by more agile programming. Additionally, the updating of software ensures new features and that the usage of the software in general is more fluent and efficient. Installing updates are fast and easy, and is often nothing more than a single click away. Thereby the effort by the consumers and citizens are on an absolute minimum, making satisficing of not doing updates hard to see. Even for the average consumer and citizen it would seem as though the aspiration level would allow for having the most secure, fast, well-functioning and up-to-date device. The alternative is nowhere attractive, and to deliberately, even with relatively limited resources of time, money, memory and cognitive abilities, avoid doing updates is not easily understood. This sparks the question: If doing updates is seemingly a no-brainer, how come a third of the consumers and citizens only occasionally update their devices?

Most likely it seems that there is simply a lack of knowledge of the need to constantly make sure to be updated with the newest software patches. With the information of the drawbacks and benefits of updates it would seem unlikely that the consumers and citizens would satisfice with an outcome of choosing not to have their devices updated. Rather, it is comprehensible that the consumer and citizen assume that the product they bought is as it should be. With most other products, such as cars, watches or furniture, the product bought does not need to be weekly updated in order to be safe to use. This contrast to the digital world is what Christian Wernberg-Touborg describes, when he talks about society not yet acknowledging the dangers within the digital sphere:

> "We do not have encoded in our DNA, what it means to be a digital citizen in a digital society, and because we do not have this, our openness to talks of it-security among citizens is limited."[85]

[85] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 1.36 min

Therefore the seemingly irrational decision of not making sure to be updated is most likely not a decision at all. The satisficing as described by Simon is thus not the reason why consumers and citizens, with imperfect information and limited resources, choose not to be updated. Rather, the case is not about imperfect information, but a complete lack of information. As Christian Wernberg-Touborg describes it, the majority of consumers and citizens do not have encoded in their DNA what it means to be digital.

This means that until consumers and citizens have encoded in their DNA that even though the piece of hardware or software seemingly work, it might be spreading virus or sharing private information. However, until this understanding becomes part of the DNA of consumes and citizens, the satisficing of having only *seemingly* well-functioning products is the aspiration level of consumers and citizens. As Wernberg-Touborg puts it:

> "We need as a society to ensure that people understand the consequences of the decisions they make when it comes to the digital."[86] And: "We have only had 20 years to learn about it-security, and that is why it is not coded into our DNA yet."[87]

When consumers and citizens eventually have their ecological rationality calibrated, the need for updates will be added to the vocabulary.

Non-rationality - Overconfidence

Where a complete lack of information on the importance of updating is a supporting satisficing within bounded rationality, the concepts of overconfidence and choice architecture argue otherwise.

Because even though updating digital products might not be customary as a part of the consumers' and citizens' DNA, looking up information on products is. When consumer and citizen purchase a car, there are several regulations that have to be met, among them insurance, driver's license and regular trips to the mechanic. This means that consumers and citizens are not unfamiliar with having to research before acquiring products.

[86] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 1.02.59 min
[87] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 25.43 min

The reason as to why consumers and citizens have not seen themselves responsible of attaining this sort of information when it comes to digital products could, according to Bhandari and Deaves, have to do with overconfidence. Consumers and citizens might credit themselves with more awareness and protection online than is actually the case. Thereby the need to seek more information and boost their understanding of the digital dangers diminishes.

As is it noted in a report done by The Danish Consumer Council in 2016, 80 % of consumers feel safe when asked about the general feeling of security online. However, when asked about specific scenarios of digital fraud like abuse of credit card information or social security numbers, around 75 % are afraid being the victims of digital fraud[88]. Thereby the confidence of consumers and citizens are high when considered broadly, but fragile when put to face with actual scenarios of digital fraud.

The discrepancy points towards overconfidence among consumers and citizens, thus supporting Bhandari and Deaves in the claim that overconfidence is among the faults of decision-makers. The self-attribution bias conceives the consumer and citizen into thinking that as long as they are not the victim of digital fraud, it is a proof of their digital skills. Conversely, the moment digital fraud is experienced; the consumer and citizens can no longer uphold the illusion of self-attribution, and are forced to objectively admit their lack of digital knowledge. Overconfidence among consumers and citizens, when only taking a stand on digital fraud as a whole, supports Bhandari and Deaves in arguing that overconfidence plays a vital role in decision-making.

Non-rationality - Choice architecture

According to choice architecture, the reason that consumers and citizens avoid updating is because decision-makers will always avoid the option which is inconvenient. By this is meant that as long as the updates take care of themselves, they are more than welcome, yet a need to attend them actively is deemed inconvenient. Thereby the lack of updates, having no real drawbacks compared to benefits, is simply a result of consumers and citizens acting along the line of Thaler, Sunstein and Balz when saying that the decision-maker often makes faulty decisions based on convenience. This theory would thus recommend as the only solution to remove the need for

[88] Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016, p. 52

consumers and citizens to reason into doing updates. Because just as it was seen on PCs when it came to installation of antivirus, a default option prevents unwanted behavior. This is supported by the fact that in Windows 7, 8 and 10, it is the default for the PC to automatically update with newer Windows patches. Thereby Windows have increased the convenience for the consumers and citizens to update, actively making not updating the inconvenient choice. Thereby the theory of Thaler, Sunstein and Balz is sustained, because until updates are the convenient choice, decision-makers will not live up to best-practice.

Bounded rationality or non-rational reasoning

Whereas the drawbacks of doing updates are almost non-existent, the challenge might lay differently. With numerous devices and software applications it takes some insight to keep track of updates. In a scenario where consumers and citizens do not have digitalization encoded in their DNA, it is not within the ecological rationality to seek out continuous updates. Thereby it is not a faulty rationality, but rationality not at play resulting in the lacking decision-making.

Yet it seems arbitrary that consumers and citizens, if not influenced by overconfidence, would not seek to gain more knowledge on the maintenance needed on digital products, just as it is done before buying a car. Furthermore, the resistance to the comprehensible, yet still inconvenient, task of updating patches that are fast, frugal and free supports Thaler, Sunstein and Balz when stating that decision-makers are lazy, basing their decisions on whatever is most convenient.

Despite digitalization not being encoded in the DNA of consumers and citizens, it is encoded in the DNA that goods bought often need maintenance. Thereby the argument of Wernberg-Touborg seems to only be valid in a scenario where consumers and citizens draw no parallels between digital products and traditional products. Because, differently from backups and antivirus, updates are closely linked to what can traditionally be defined as reparations or maintenance. This makes updates stand out, because it seems that the intuitive behavioral pattern should be to do updates, however, this is not the case for a third of consumers and citizens.

Rather, it seems somewhat overconfident that consumers and citizens simply assume their devices to be secure. In combination with a decision-maker acting within accordance of a choice architecture, where convenience is king, the decision-makers ecological rationality seems to be affected by non-rational tendencies, even when counting in the lack of being accustomed to

digitalization. Thereby the lack of doing updates support theories of non-rational decision-making, because even within ecological rationality and satisficing, it is seems that the decision-makers are going against the assumed satisficing.

No skepticism and (no) rationality

The advice – Have a healthy skepticism

Although having a healthy skepticism is not connected purely to it-security, it is nonetheless always among the most frequented piece of advice. The chain of thought by experts is that with a healthy skepticism online, consumers and citizens will be inclined to dig further into the understanding of digital threats, and thereby possibly take to them some of the other recommended pieces of it-advice. Having a healthy skepticism is, however, hard to teach and hard to measure. The surveys done on it-security do not ask about whether or not the participants consider themselves having a healthy skepticism online. It is therefore the roaring number of cases of reported digital fraud that most visibly icons the development within digital fraud. Consumers and citizens are experiencing an increase in digital fraud, contrary to the decrease in traditional crime. This suggests a lacking ability of consumers and citizens to skeptically see through the traps online, this is especially dire in Scandinavian societies who are relying on trust[89]. This is why a healthy skepticism online could find merit in hope of transferring the positive tendency from the traditional crime.

Rationality - Bounded rationality

Having a healthy skepticism is not something that a software provider can supply. No backup, antivirus or update can give the consumers and citizens the ability to be skeptic at the right moment. Attaining a healthy skepticism online is about developing and maintaining the toolbox that allows the consumers and citizens to be skeptic. This toolbox has been developed in the physical world for centuries, but as previously described by Christian Wernberg-Touborg, the coming of the digital era is relatively new, prompting digital security to be a new field of DNA-encoding not yet implemented. Wernberg-Touborg furthermore describes how this physical DNA-

[89] Tillidssamfundet Danmark, Børsen, Peter Holdt Christensen, Ph.D at Copenhagen Business School, October 2006. Available at: http://borsen.dk/nyheder/avisen/artikel/12/1830955/artikel.html

encoding is lacking within the digital sphere, thus making consumers and citizens more vulnerable to digital fraud:

> "When we have interpersonal communication, there are tons of coding and comprehensive understanding of body language, voice levels and gestures involved. The moment you enter the digital sphere instead, all of this is detached, and this allows you to be easier seduced in the digital world."[90]

As Wernberg-Touborg puts it, when there are no tells of when to be skeptic or not, such as aggressive body language or raised voice, it becomes difficult for the average citizen to be skeptic at the right moments. This lack of information results in the reasoning to be based on imperfect information, thus resulting in a situation of bounded rationality. This might result in citizens and consumers not being skeptic, thus making decision-makers satisfyingly suffice with making decisions that wrongfully assumes harmless intensions online. This barrier between physical and digital understanding of behavior prevents faster implementation of a healthy skepticism in the decision-making of consumers and citizens digitally.

For consumers and citizens the satisficing is about being able to weigh the information available, and then make a decision that, in the best possible way, balances the limited time, money, memory and cognitive abilities. The satisficing of being skeptical online is thus a balance of continuously being able make decisions, whilst not possessing the tools needed to sort through the fed information. In a situation where the available toolbox needed in order to be skeptical is lacking, the consumers and citizens are forced to make decisions within a faulty ecological rationality.

It is not an option to opt out of digitalization, but it is neither an option to make decisions based on sufficient information. Thereby the consumer and citizen are forced to make naive decisions. Nonetheless, considering the difficulties of achieving the information needed to be healthy skeptical, the lack of skepticism supports Simon and Becker when arguing that decision-makers will always satisfice with bounded rationality and imperfect information. Summarized, it can be said that the aspiration level among decision-makers declines because of the overarching need of

[90] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 26.23 min

consumers and citizens to be deliverable in decisions. Thereby the ecological rationality among consumers and citizens is that digitalization will uninterrupted go on, despite rising numbers of incidents of digital fraud, forcing decisions despite the lack of foundation for healthy skepticism.

Non-rationality - Cognitive dissonance

The lack of a sufficient healthy skepticism among consumers and citizens could, however, also be argued to support non-rational influences such as cognitive dissonance and emotional impact. It is most important to recollect that within cognitive dissonance decision-makers always want to be comfortable. This means that whenever a decision has to be made, the decision-maker is inclined to make the decision according to the moral beliefs, and to what is accepted and recognized by society as proper behavior. For it-security this means that when the consumers and citizens are engaging digitally, it might not be attractive to accept the threat of digital fraud at all, as Peter Kruize puts it:

> "The mental space that needs to be created, in order to recognize that the problem [of digital fraud] is so big that it needs to be acted on, is demanding. You would have to be afraid all the time, and therefore it is not attractive to admit that there is a risk."[91]

In order to fully take on the responsibility of being skeptic when acting online, the consumer and citizen would need to fully recognize the severe degree risk of being the victim of digital fraud. This admittance is highly stressful and demanding, and is therefore intuitively unattractive for the decision-maker that is seeking to be comfortable[92]. Instead of accepting to be indulging in immoral behavior, it is more attractive to the decision-maker influenced by cognitive dissonance to change beliefs, and thus denying the need to change behavioral patterns[93]. This is exactly what Peter Kruize elaborates on when talking about the unwillingness of consumers and citizens to have anything to do with the digital threats:

[91] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 11.28 min
[92] Cognitive Dissonance and Social Change, Matthew Rabin, Journal of Economic Behavior and Organization, University of California at Berkeley, 1992, p. 178
[93] Cognitive Dissonance and Social Change, Matthew Rabin, Journal of Economic Behavior and Organization, University of California at Berkeley, 1992, p. 178

> "The threat is being looked upon differently, and some see the threat level differently than others, but the general opinion is that it is uninteresting and unwanted to have anything to do with the digital threat."[94]

The consumers and citizens lack of skepticism is thus not a result of imperfect information and bounded rationality. It is rather a result of cognitive dissonance invoking the decision-makers to deny the actuality of the need for proper digital protection and security. Thereby the non-prevalent healthy skepticism backs Matthew Rabin and Peter Kruize in stating that it is more comfortable to simply deny the existence of a digital threat, than to accept the threat and then admit immoral and wrongful behavior. The missing skepticism thus becomes a way for the decision-maker to adhere to the conformability of acting within the socially accepted behavior.

Non-rationality - Emotions

Supporting the non-rational influence on decision-making is Jon Elster, who argues that emotions affect the decision-weights. This results in decisions where feelings such as impatience, anger or frustration plays a role. These feelings might be irrational, but they are none the less affecting the reasoning of decision-makers, in other words: emotions shape preferences. This is also something Christian Wernberg-Touborg has experienced in the debate of digitalization:

> "Some allows their feelings to go ahead, and then it becomes every emotional, and then it becomes about doing something for the sake of it. Oppositely others argue constantly in a negative connotation, without rationally considering whether or not their position is correct […] the debate becomes tremendously emotional."[95]

As Wernberg-Touborg puts it, emotions play an incremental role in the development of the digital sphere including it-security. Whether decisions are made by consumers and citizens with a healthy skepticism in mind thus depends on emotions tipping the balance either way.

For some consumers and citizens the positive feelings connected with the opportunities of the infinite digital world might result in a refusal to be critical regarding the digital life. This prevents segments of consumers and citizens to make rational decision with a healthy skepticism. For

[94] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 12.41 min
[95] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 55.18 min

others fear and anxiety might be the reason that they go around digitalization with an overshadowing skepticism, preventing any of the benefits of the digital life. The two sites of the table might be equally damaging in order to have a well-functioning and healthy skepticism that supports digitalization and digital protection:

> "Emotions play a role when it comes to what kind of society is wanted. Some wants to digitalize everything as soon as possible, while others consider it to be the end of the world as we know it."[96]

Whether or not the consumer and citizen is overly negative or overly positive does not influence that, according to Christian Wernberg-Touborg, the emotional impact greatly affects the decision-making of consumers and citizens, when it comes to the level of skepticism.

Bounded rationality or non-rational reasoning

The missing healthy skepticism has been argued to be a result of satisficing, but also as a product of cognitive dissonance and emotions affecting decision-making. The argument that the missing healthy skepticism is caused by what Simon and Becker describes as bounded rationality is backed by the fact that digitalization has not yet been encoded in the DNA of consumers and citizens. Furthermore, it seems rational that in a digitalized society, it is not an option to stop making decisions online. This justifies to the consumers and citizens that a satisficing result is to make decisions without a healthy skepticism.

Conversely, the cognitive discomfort of allowing oneself to feel insecure in the digital sphere is an argument where Matthew Rabin and Peter Kruize agree. This is because decision-makers, here being consumers and citizens, are uninterested in creating the mental space for understanding digital fraud. The discomfort of acknowledging that digital fraud demands behavioral change results in consumers and citizens denying digital insecurity. By denying being afraid of digital fraud, the consumers and citizens thus reinforces the critique of not being sufficiently skeptic within the digital sphere, because allowing skepticism would demand mental space. Combined with the emotional impact on decision-making, making consumers and citizens either overly

[96] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 54.29 min

positive or negative, contributes to the story of the lacking skepticism being a result of non-rational notions such as cognitive dissonance and emotions.

However, for the case of the lacking skepticism, it is noteworthy to consider the time of entry for the concepts of the rational and non-rational influences on decision-making. Whereas it is reasonable that consumers and citizens maintain the need to be able to conduct decisions, it does not change that the decision-makers here are going against what they are told to do: only make decisions on sufficient information. By ignoring this advice, the decision-makers are being challenged on their ecological rationality. This is by any means unpleasant, as it is a common trait wanting to be understood. Therefore the theory of emotions and cognitive dissonance, with an underlying assumption of non-rationality, is not sustained in the decision-making itself, but in the following processes.

By allowing non-rational tendencies, such as emotions and cognitive dissonance, to disguise the actual confrontation of the ecological rationality, the non-rationality concepts work in extension of satisficing. Emotions and cognitive dissonance are thereby delivering comfort, relieving decision-makers of frustration on having their ecological rationality question in situation where no real alternatives are available.

No unique passwords and (no) rationality

The advice – Use unique passwords

When consumers and citizens choose their passwords it is far too often obvious ones. Around 50% choose password within the 25 most common sequences of numbers and/or letters, whereas others choose familiar combinations of names, places and birthdays[97]. These combinations are for it-criminals easy to guess, as they have only need access to public databases, such as Facebook, in order to make competent guesses. With a combination of random numbers and letters, or by using a so-called piece of software called a 'passwordmanager', the consumer and citizen can greatly improve the robustness of one's digital security. Therefore the advice would be to simply use unique passwords, or to introduce a passwordmanager into the everyday usage of digital

[97] Do you have one of the most common passwords?, The Telegraph, James Titcomb, March 2016. Available at: http://www.telegraph.co.uk/technology/2016/01/26/most-common-passwords-revealed---and-theyre-ridiculously-easy-to/

services. This is, however, as mentioned, not the case, and therefore it-experts' advice is not being followed by consumers and citizens.

Rationality - Bounded rationality

For consumers and citizens the way to make sure their passwords are hard to guess is somewhat intuitive: have unique passwords. It does not take much thought to follow the logic that having the same key for all doors is troublesome. If this universal key would be stolen in the physical world, the thief can not only access the house, but also drive away in the car. This is why most people maintain different keys, and often have their car keys on a separate chain than the keys for their house.

However, in the digital life, it is not as simple as having a number of different physical keys. With digital logins there exist no physical token used to access the digital services. The username and password have to be remembered. To the average digital citizen this means that dozens of usernames and passwords have to be memorized, along with what logins information suits the correct platform. Some might be more important than others, but it is nonetheless frustrating when the login is forgotten, thus making the booking of for instance a dentist appointment difficult and time consuming. Therefore it seems that the consumer and citizen most likely is perpetuating in repetitive use of the same passwords in order to satisfy their everyday needs. With limited available time and memory, consumers and citizens are simply not being able to remember 50+ combinations of unique passwords.

When consumers and citizens avoid spending time on memorizing passwords or inconvenient passwordmanager, it seems to prove the thoughts of Simon and Becker, when they argue that decision-makers satisfice within the imperfect information available to them. When it comes as a surprise that the consumers and citizens refrain from having unique passwords, it is a sign of a lack of understanding of the process of satisficing by it-experts. When not being able to, or in desire of, continuously remembering dozens of unique passwords, it is due to the fact that the consumers' and citizens' aspiration level has been met. This is because the satisficing is based on an aspiration level being met when the login is to be remembered. The consumers and citizens only secondly focus on the passwords as a means of digital protection. By doing this sort of satisficing the consumers and citizens follow a rule of thumb that is making their daily routines doable.

Having unique logins might be wise when looking at the broader scheme of things, because seemingly innocent logins can pose security threats when connected in large scale. However, with limited information available, the reasoning of consumers and citizens connects well with the thought that making decisions is a balance between what suffices and what is satisfying. In doing so, the ecological rationality is sound as long as the password can be remembered. This rationality might not be focused on it-protection, but it is backing Simon and Becker when arguing that the individual is bounded rational. The rationality at play might be controversial, but it is nonetheless rationality at play.

This acknowledgement of several rationalities being at play is one that Peter Kruize supports. When talking about the role of the citizens in the digital protection Peter Kruize express doubt if whether this is the right way to go. According to Kruize the potential within making sure the citizens have the correct mindset is difficult. Instead focus should be on the framing, wherein the correct rationality would be unavoidable to the consumers and citizens:

> "Focus is a lot about what the citizens are supposed to do or not supposed to do, and I am quite skeptic to this being the way to go. I think focus should be more about the digital framework of the digital life, because by changing this I see the greatest potential for chance."[98]

Peter Kruize supports Simon and Becker in saying that consumers and citizens only have access to bounded rationality. In order to make significant change, it is needed to change the framework around the digital life, because only by doing so, can the wanted behavioral patterns be obtained. If allowed, the consumers and citizens will through the imperfect information available satisfice, thus maybe making decisions on basis of an unwanted rationality.

Non-rationality - Overconfidence

The lack of emphasis on having unique passwords was depicted by Simon and Becker as a result of imperfect information and satisficing. Going against this theory is Bhandari and Deaves, who connects overconfidence to poor decision-making. The reason consumers and citizens find themselves using the same patterns for password-generating can, following the theory of Gokul Bhandari and Richard Deaves, be a result of self-attribution bias. When overestimating the skills in

[98] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 14.09 min

creating passwords, the consumers and citizens' end up making passwords that broadly correlate within the same pattern. The general easiness of which it-criminals can go to the task of guessing passwords, with a majority of passwords following the same patterns, supports Bhandari and Deaves in their views on overconfidence affecting decision-making.

Furthermore, as outlined by Bhandari and Deaves, there is empirical data pointing to seniority boosting overconfidence. This is especially dire in the situation where the relatively new phenomenon of creating digital passwords is not encoded in the DNA of consumers and citizens:

> "Little children, adults and elders are on the same level when it comes to understanding the digital world, whereas in the physical world it is exactly opposite, because the elder you get the more information you have"[99]

Here Christian Wernberg-Touborg outlines how age has not yet improved the understanding of the digital world. Combined with the growing overconfidence with seniority, this makes to a combination of increasingly overconfident adults and elders not realistically assessing their digital decision-making. In the context of creating solid passwords, the consequence can be that the overconfidence in password-generating is especially prevalent among older generations.

The obvious pattern upon which passwords are constructed backs Bhandari and Deaves when stating that decision-makers are overconfident. If realistically assessing the ability to construct solid passwords, consumers and citizens would likely indulge in more intricate password generating. Furthermore, the pattern of seniority boosting overconfidence would suggest that the issue of inadequate password combinations is worsening by age.

Non-rationality - Emotions

Whether emotions play a role in decision-making, including in deciding to have unique passwords or not, is something Jon Elster would argue. The feelings of fear, insecurity, invulnerability or optimism are something that, according to Elster, affects decision-making. For generating of passwords the attention put into having unique passwords for every service is something that would therefore be affected by the emotions of the decision-maker.

[99] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 51:01 min

As described in the previous section, overconfidence could be a source of why consumers and citizens construct passwords following the same patterns. Besides considering the used password as being more unique than the case is, the conceived chance of being attacked by it-criminals is contributing to whether or not passwords need to be unique. Because according to Peter Kruize, the belief of the consumers and citizens is just as likely to affect deciding whether or not to have a unique password. Supporting the theory of Elster, the non-rational reliance on feelings to influence decision-making is something that Peter Kruize supports when stating that the beliefs of consumers and citizens affect decision-making:

> "People make decision out of individual regards, and they make decision based on their own conviction and convenience of not being the next one hit by it-criminals. They think that yes, sure, I might not be entirely certain if it is dangerous [to be the target of digital fraud], but I don't believe it is, and I don't think it will happen to me either way."[100]

Peter Kruize supports the foundations of Elster when he argues that the sentimental conviction of the consumers and citizens are influencing the understanding of being hit by digital fraud. This irrational 'belief' of not being hit by digital fraud is thus manipulating what experts on the field exert. Thereby, according to Elster and Kruize, the methods to make consumers and citizens introduce unique password is based on an assumption of logic that forgets the role of belief in decision-making. Based upon the majority of consumers and citizens reusing passwords, Elster and Kruize are boosted in their notion that it-experts need to consider the emotional beliefs in order to change the behavioral patterns of consumers and citizens when it comes to unique passwords.

Bounded rationality or non-rational reasoning

As Simon and Becker puts it, the decision-maker satisfices. For passwords the satisficing is proved by consumers and citizens accepting generic passwords in order to remember the 50+ logins many face. The satisficing thus becomes to suffice clear when the key feature of the password changes from giving security to giving access. That this is the ecological rationality of the consumers and citizens is thus supported by the fact that the majority of consumers and citizens make use of repetitive passwords, despite the intuitive disadvantages.

[100] Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen, 49.40 min

Both overconfidence (in the form of self-attribution bias) and emotional 'belief' (in that digital fraud is not a threat) affecting decision-making is relevant to include in the discussion. This is especially relevant when discussing the attention put into even the repeated passwords. Likely, overconfidence and emotions is resulting in decision-makers paying less attention to making even the repeated passwords difficult to guess. Yet, it seems logic to assume that if there was a conceivable system of memorizing the 50+ unique passwords and logins, the underlying assumptions of decision-makers being overconfident and affected by emotions cannot explain why such a system would not be taken into use.

Rather, it seems that overarching flaw in the system of passwords and logins is that it is simply not compatible with human limitations. Thereby the case of repetitive passwords strongly supports Simon and Becker in their theory of bounded rationality, where limited memory is influencing decision-making. The case of repetitive use of passwords heavily outlines that both it-experts, consumers and citizens can act rationally, but with different rationales. In total, that ecological rationality explains the lack of unique password from consumers and citizens seems to be extremely reasonable when considering bounded rationality and satisficing.

Conclusion: Competing ecological rationalities

The role of rationality in decision-making, symbolized by how consumers and citizens were not following the advice of it-experts, was the onset of the dissertation. To discuss rationality in decision-making two segments of theoretical concepts were highlighted. These were divided into rationality and non-rationality theories. Throughout the analysis, the case of it-security was used to highlight and test the concepts of decision-making. This was done to underline assumptions and contradictions between the concepts of rationality and non-rationality. The case analysis thus has resulted in the following theoretical conclusions:

The advice of it-experts is through this dissertation assumed to be rational. By rational is meant that there is a correlation between the wanted behavior and the objective findings of digital fraud. It is assumed that the advice will help to protect the consumers and citizens, just as it is assumed that there is an adherence between obstacle and solution. However, this rationality is not necessarily shared by consumers and citizens.

According to Herbert Simon and Gary Becker, the way of decision-makers is that of bounded rationality. The rationality of the decision-maker is limited by circumstances, but it is nonetheless rationality within a limited ecology. As long as this is the case, whenever stakeholder managers are trying to change behavior, it is through the lens of rationality it has to be done. Simon and Becker are not dreaming of perfect rationality with perfect information, but whilst considering the limitations of rationality, the way decisions are made is still through rational reasoning. As described by Gigerenzer and Gaissmaier, it is the ecological rationality defining what action is rational.

For instance, to it-experts, the ecological rationality is to tell consumers and citizens to have unique passwords on all their services. To consumers and citizens this might be completely irrational. With limited time and memory the consumers and citizens, defying having unique passwords, have most likely come to the conclusion that the rationality between obstacle and solution was out of tune. The perceived consequences of having the same password for seemingly unimportant services does, from view of consumers and citizens, not prove sufficient to have the inconvenience of memorizing 50+ unique passwords. This logic is flawed in the eyes of the educated it-professional, who is able to see the bigger picture, but in the everyday lives of

consumers and citizens, there is simply not a connection between the benefits and drawbacks of unique passwords.

Furthermore, the recent emergence of digital fraud has consistently proven to be a valid argument as to why backups, antivirus and updating are yet to be completely normalized. As Christian Wernberg-Touborg puts it, it is necessary to have digital protection included in the ecological rationality, or DNA, of the consumers and citizens. Before this happens, the bounded rationality of the decision-maker will prevent the wanted behavior.

Likewise, the argumentation that choosing the convenient default option is a proof of non-rational decision-making is controversial. Just as likely, it can be argued that by choosing the default option, the decision-maker is optimizing by using the heuristics of assuming that the default option is the most favorable choice. On almost all other facets of life, the decision-makers will be facing options where someone else has already defined the best option as the default option. This is for instance the case when the government ensures that the cars we drive, the food we eat and the cloth we wear are not filled with toxic chemicals or falling apart instantly. On these areas, the decision-makers are rationally assuming that the standards of goods in the supermarket or the store have all passed certain benchmarks. This ecological rationality, rationally assuming a choice architecture delivering little chance of making poor choices, is thus making it unfrugal to spend already limited resources on researching if default options live up to required standards.

The absent skepticism could be a point of critique, but as it has been showed in the analysis, it is nonetheless hard to possess a healthy skepticism when the knowledge needed to do so, in the current state of affairs, vastly surpass the cognitive abilities of the human mind. In that way, the satisficing of the decision-maker is a system of being able to make decisions despite of imperfect information. It is, in the concrete case of digital safety, therefore rational of consumers and citizens to consist in making decisions, despite not being fully aware of the all the digital threats. Furthermore, as described, there is a continuous stream of advice flowing from experts on everything from food, exercise or sex. To be completely open to every suggestion on how to behave would make the decision-maker unable to make any decisions, and indeed goes against the advice of being healthily skeptical.

Non-rationality giving comfort

That decision-makers are influenced by non-rational tendencies is, however, also backed by the analysis. There are consistent signs of consumers and citizens seeking convenience and comfort, often through self-attribution bias or by mental accounting. There are also signs that the consumers and citizens are behaving according to Kahneman and Tversky when not understanding the risk involved with loss-aversion.

Of the pieces of advice analyzed, it is especially the lack of updates that are going against the theory of bounded rationality. Where the others pieces of advice seems to support that it is most likely the ecological rationality preventing advised behavior, it is difficult to find proof that the theory of ecological rationality can explain the lack of updates. Despite updates of software being a relatively new phenomenon, it is nothing new that acquired goods need maintenance. To have an ecological rationality among decision-makers that is resulting in behavior going against the traditional patterns developed over centuries is not convincing. Contrary to the theory of bounded rationality it does seem more likely that the explanations of overconfidence and choice architecture are more deliverable in answers.

Yet, it does not change the overall picture, where most behavior by consumers and citizens can be explained through a lack of computational capacities resulting in locally based ecological rationalities.

Because when the seemingly non-rational behavior of gambling with it-security becomes a way to support it-criminals, it is cynical to demand that consumers and citizens include this consideration in their ecological rationality. Instead, it seems that the tendencies of non-rational influences become more of a supportive element to already unwanted behavior. The overconfidence, mental accounting and cognitive dissonance thus become ways of increasing comfort, something that is rational wanting to obtain, especially in situations where recommended behavior is incompatible with the ecological rationality of the decision-maker. Specifically the non-rationality concepts allows for the consumers and citizens to defend their ecological rationality, despite not doing so by rational argumentation. The case thereby points to the fact that the non-rational tendencies functions as an a posteriori way of increasing comfort, after satisficing within the ecological rationality has been sanctioned.

Outlining that bounded rationality is not being overshadowed by non-rational tendencies is the fact that behavior changes along with information. As previously mentioned, data suggests that 96% of consumers and citizens change behavior after having their digital security threatened[101]. This serves as ratification that decision-makers change of behavior when faced with changes in their ecological rationality. The imperfect information and cognitive limitations thereby become apparent as the most crucial reason as to why decision-makers do not follow best-practice. The moment the ecological rationality becomes influenced by a heavy change in the surroundings, behavior changes, and the new information becomes part of the behavioral patterns of the decision-maker. However, with limited resources, the decision-maker cannot change behavior a priori to a change in the balance behind the satisficing. The analysis therefore provides backing to ecological rationality being the most best describing explanation to the unwanted discrepancy between the actual and wanted behavior of decision-makers and stakeholder managers, in this case between consumers, citizens and it-experts.

Thereby, the non-rational influences on decision-making are not necessarily in opposition to bounded rationality, rather they seem to function as a way for decision-makers to increase comfort in a situation where satisficing is demanded. This is because satisficing is in its essence a suboptimal solution. To satisfyingly accept decisions that, based on the aspiration level, simply suffice does not intuitively make consumers and citizens content. However, with contribution from a little overconfidence, some mental accounting, cognitive dissonance and emotions, the decision-makers eases the burden of accepting their satisficing as a less than suboptimal outcome.

The role of rationality in decision-making

The purpose of the dissertation was to answer the following:

1. *What role is rationality playing in decision-making of stakeholders, and how is rationality best considered in stakeholder management deliberations?*

2. *Can rationality theories of bounded rationality, satisficing and ecological rationality better explain decision-making, than non-rationality theories of decision-making focusing on mental accounting, overconfidence, prospect theory, cognitive dissonance, emotions and choice architecture?*

[101] Danskernes Informationssikkerhed, DKCERT, DEIC, different authors, 2017, p. 24

In conclusion, rationality, in the form of ecological rationality, seems to have a dominating role in the decision-making of stakeholders, in this case analysis the consumers and citizens. The non-rational tendencies among decision-makers can, on basis of the current case analysis, for the most part be explained by competing ecological rationalities. The concepts of non-rational decision-making instead present themselves to be giving comfort and convenience in situations of satisficing. The concepts of bounded rationality, satisficing and ecological rationality most successfully explain what is preventing stakeholder managers from achieving their goals. Therefore, competing ecological rationalities need to be considered in the process of stakeholder management. Nonetheless, it is important to note that the case analysis still suggests non-rationality to be influential in the process of accepting satisficing as a decision-model. Thereby both strains of theory contribute to understanding the role of rationality in decision-making, from an a priori and a posteriori perspective.

Perspective: The responsibility of the stakeholder managers

Almost on a weekly basis there exist new initiatives on it-security from stakeholder managers. However, with the conclusion that it is ecological rationality resulting in a discrepancy between decision-makers and stakeholder managers, it becomes clear that in order to boost it-security, the confrontational rationalities have to be aligned.

Until now, the discussion has been about the best way to achieve the correct behavior of individual decision-makers on it-security. Contrary to this, when ecological rationalities simply do not correlate, it becomes clear that it-security has to be reached elsewise. Rather than focusing on individuals, the responsibility should be manifested on stakeholder managers, who on a large scale should take on them to meet the rising demand of taking digital security. One of the supporters of this is Christian Wernberg-Touborg:

> "The politicians need to begin making standards of it-security, but not only Danish politicians. We live in a globalized world, and therefore we need a globalized technology-treaty, where we will have general rules and understandings of how to use digital mechanisms, and where we protect privacy. It should be a digital version of the human rights charter."[102]

Wernberg-touborg does not lay his focus on the individual; instead he focuses on the responsibility of the politicians as the main stakeholder managers on it-security. The reason for this might be that Christian Wernberg-Touborg has accepted that it will never be feasible to fully agree on a single ecological rationality. The rationality of the decision-makers will always be limited by bounded rationality and satisficing resulting in confronting rationalities.

This is supported by reports signifying that newer generations of digital users does not have a better understanding of the digital world. The so-called digital natives, who have been born in a digitalized world, do not express impressive competencies when it comes to digital skills[103]. Rather, digitally native generations only show competencies within the limited digital sphere used regularly. This means that newer generations excel in social media, Google search and taking to

[102] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 38.42 min
[103] Digitale elever er knap så indfødte, Camilla Mehlsen, December 2014, p. 1

them new technologies. However, neither of these skills ensures that coming generations of consumers and citizens will be fitted with the necessary abilities to improve it-security.

The needed alignment of rationalities between it-experts, consumers and citizens is therefore not automatically a bi-product of increased use of digital devices. Oppositely, reports strongly points towards younger generations having increasing difficulties of being critical to information[104]. This could in worse case scenarios result in new generations of consumers and citizens accepting terms without reading them, and who are carelessly clicking links and downloading software.

If this development continues, the DNA-encoding of digital security is not one that can simply be expected to arise. The ecological rationality might change according to rising numbers of people being experiencing digital fraud, but there is no guarantee that the changing of the ecological rationality can keep up with new initiatives from it-criminals.

This is most likely why both Peter Kruize and Christian Wernberg-Touborg agree that the future of it-security should not lie on the shoulders of individual consumers and citizens. Instead, the responsibility is to be placed with politicians and other stakeholder managers. This group needs to ensure standards of it-security, not allowing local ecological rationalities to prevent correct behavior of digital protection among consumers and citizens. One way to go about this is nudging, which Christian Wernberg-Touborg expresses support of:

> "We had a suggestion saying that in order to access public services, consumers and citizens would have to live up to specific requirements of digital security. This could involve updating software and installing antivirus … the idea was good because it involved nudging the citizen into changing behavior."[105]

In the scenario described by Wernberg-Touborg, it is in the wish to be a part of the digitalized society those consumers and citizens will live up to the standards of it-experts. Nudging will not result in the correct behavior of consumers and citizens due to a sharing and alignment of

[104] Bad News: 80% of Students can't Tell the Difference Between Real and Fake News, ScienceAlert, Fiona MacDonald, December 2016.
Available at: http://www.sciencealert.com/bad-news-study-finds-80-of-students-can-t-tell-the-difference-between-real-and-fake-news

[105] Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen, 1.01.44

rationalities, since the ecological rationality of the decision-making consumers and citizens will not suddenly compulsory correlate with the rationality of it-experts. This is, however, not needed because it is through nudging possible to come by it-security as a side effect. Choice architecture thus becomes relevant not because decision-makers are necessarily lazy and convenience seeking, but because choice architecture makes obsolete the need to agree on the same ecological rationality. This sort of pre-deciding the accepted choices, upon which the decision-maker then freely can make a selection, is closely linked to the concept of liberal paternalism. Liberal paternalism is to softly nudge the decision-maker to go along the paternalistically ordained path[106].

Nudging is thus ideal because a well-designed choice architecture allows structuring of correct behavior without sharing the same ecological rationality. Through nudging it becomes irrelevant to share the same ecological rationality; it is, however, needed to understand the ecological rationality of decision-makers in order to do so. Only then it becomes possible to bypass unwanted behavior by exploiting the rationality of decision-makers into making satisficing that fit the agenda of stakeholder managers.

On the field of it-security this could be to make updates mandatory, or to refuse access to public websites without proper antivirus installed. Furthermore, backups should be preset on new computers, just as passwords would be needed to uphold more demands before being accepted by digital services. The healthy skepticism could be acquired by affecting the ecological rationality by demanding compulsory courses to be passed before being able to access public websites. This combination of nudging and not-allowing local ecological rationalities to affect decision-making is, based upon the conclusions from the case analysis, the optimal approach of stakeholder managers wanting to count in the role of rationality.

[106] Liberal Paternalism, Richard M. Thaler and Cass R. Sunstein, AEA Papers and Proceedings, May 2003, p. 175

Bibliography

Reports

- Fra barndommens gade til cyberspace, Flemming Balvig, Det Kriminalpræventive Råd, 2017
- Trendrapport 2016, DKCERT - DEIC, different authors, 2016
- The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context, European Economic and Social Committee, EU, 2017
- Digital Tryghed – De væsentligste digitale udfordringer for forbrugerne i Danmark, The Danish Consumer Council, January 2016
- Digitale elever er knap så indfødte, Camilla Mehlsen, December 2014
- Kriminalitet i en digitaliseret verden, Peter Kruize, Faculty of Law, October 2013
- Online security survey, The Danish Consumer Council, March 2017
- Online security survey, IDA, 2017
- Danskernes Informationssikkerhed, DKCERT, DEIC, different authors, 2017
- The Most Common Passwords of 2016, Keeper Security, 2016

Interviews

- Interview in June 2017, Peter Kruize, Lector in criminology, Faculty of Law, University of Copenhagen
- Interview in June 2017, Christian Wernberg-Touborg, Board member of The Council for Digital Security and Chairman of the security committee at IT-Branchen

Theory

- Five Misunderstandings About Case-study Research, Bent Flyvbjerg, Aalborg University, 2006
- Introduktion til et håndværk, Steinar Kvale and Svend Brinkmann, Hans Reitsels Forlag, 2008, p. 167
- Metoder i statskundskab, Lotte Bøgh Andersen, Kasper Møller Hansen and Robert Klemmensen, Hans Reitzels Forlag, 2010, p. 20-41, 100-105 and 145-150.
- Becker on Ewald on Foucault on Becker, University of Chicago, 2012
- Rational Decision-making in Business Organizations, Herbert Simon, Nobel Prize Lecture, Carnegie-Mellon University, 1978
- The Economic Way of Looking at Behavior, Gary Becker, Nobel Prize Lecture, University of Chicago and Hoover Institution, 1992
- Heuristic Decision Making, Gerd Gigerenzer & Wolfgang Gaissmaier, Annual Review of Psychology, Max Planck Institute for Human Development, 2011
- Invest now, drink later, spend never: On the mental accounting of delayed consumption, Eldar Shafir and Richard H. Thaler, Journal of Economic Psychology, Princeton University, 2006
- The demographics of Overconfidence, Gokul Bhandari and Richard Deaves, The journal of Behavioral Finance, The Institute of Behavioral Finance, 2006
- The Dynamics of Overconfidence: Evidence from Stock Market Forecasters, Richard Deaves, Erik Lüders and Michael Schröder, Journal of Economic Behavior & Organization, 2010
- Prospect Theory: An analysis of Decision under Risk, Daniel Kahneman and Amos Tversky, The Economic Society, 1979
- Cognitive Dissonance and Social Change, Matthew Rabin, Journal of Economic Behavior and Organization, University of California at Berkeley, 1992

- Emotions and Economic Theory, Jon Elster, Journal of Economic Literature, American Economic Association, 1998
- Choice Architecture, Richard M. Thaler, Cass R. Sunstein and John P. Balz, Department of Political Science, University of Chicago, 2010
- Liberal Paternalism, Richard M. Thaler and Cass R. Sunstein, AEA Papers and Proceedings, May 2003

Articles

- Internet of Things, Tado, 2017. Available at: https://www.tado.com/sg/internet-of-things
- Fraud, Merriam-Webster Dictionary. Available at: https://www.merriam-webster.com/dictionary/fraud
- Flere bedragerier, færre brud, Danmarks Statistik, February 2017. Available at: http://www.dst.dk/da/Statistik/nyt/NytHtml?cid=23527
- Flere databedragerier still krav til brugernes it-sikkerhed, Danmarks Statistik, March 2017. Available at: http://www.dst.dk/da/Statistik/bagtal/2017/2017-03-27-flere-databedragerier-stiller-krav-til-brugernes-it-sikkerhed
- Cyber- og informationssikkerhed: Danmarks digitale sikkerhed skal styrkes, Samfundsdesign, Per Roholt, January 2017 . Available at: https://samfundsdesign.dk/administration/datasikkerhed/cyber--og-informationssikkerhedsstrategi/
- De kæmper mod hackere, pædofile og elektroniske lommetyve, Dansk Politi, Tania Kejser, June 2016. Available at: http://www.dansk-politi.dk/artikler/2016/juni/de-kaemper-mod-hackere-paedofile-og-elektroniske-lommetyve
- 10 råd til sikker pc-brug, Digitaliseringsstyrelsen. Available at: https://www.borger.dk/internet-og-sikkerhed/Sikker-selvbetjening/Se-10-gode-raad
- 10 gode råd til bedre sikkerhed, C-Cure. Available at: https://www.c-cure.dk/for-private/10-gode-raad-til-bedre-sikkerhed/
- 10 tips til bedre IT-sikkerhed, Ekstra Bladet, Thomas Gösta Svensson, Anders Ejbye-Ernst, Alexander Sokoler, Steffen Moses og Jens Christian Hillerup, August 2015. Available at: http://ekstrabladet.dk/nyheder/friadgang/guide-10-tips-til-bedre-it-sikkerhed/5698949
- Herbert Simon, The Economist, March 2009. Available at: http://www.economist.com/node/13350892
- Dansk e-handel boomer, Business Danmark, Peter Hjorth, September 2016. Available at: http://www.businessdanmark.dk/Inbusiness-forside/InBusiness-artikelarkiv/2016/Q3/Dansk-e-handel-boomer/
- Ofre for net-tyveri langer ud efter politiets jagt på digitale tyve, Danmarks Radio, Laura Marie Sørensen, October 2015. Available at: https://www.dr.dk/nyheder/indland/ofre-net-tyveri-langer-ud-efter-politiets-jagt-paa-digitale-tyve
- Stor sikkerhedstest: Her er det bedste antivirus-program lige nu, ComputerWorld, Nicolai Devantier, March 2016. Available at: https://www.computerworld.dk/art/236634/stor-sikkerhedstest-her-er-det-bedste-antivirus-program-lige-nu
- How to spot a 'Free iPhone' (or 'Free iPad') scam, Macworld, Lucy Hattersley, September 2015. Available at: http://www.macworld.co.uk/feature/iphone/free-iphone-ipad-scam-fake-auction-site-facebook-3608522/
- Reusing Passwords on Multiple Sites, Center for Internet Security, June 2016. Available at: https://www.cisecurity.org/reusing-passwords-on-multiple-sites/
- Do you have one of the most common passwords?, The Telegraph, James Titcomb, March 2016. Available at: http://www.telegraph.co.uk/technology/2016/01/26/most-common-passwords-revealed---and-theyre-ridiculously-easy-to/
- Dropbox hack leads to leaking of 68m user passwords on the internet, The Guardian, Samuel Gibbs, August 2016. Available at: https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
- Cyberangreb kan koste trecifret milliardbekøb, Fyens Stiftstidende, Ritzau, July 2017. Available at: http://www.fyens.dk/erhverv/Cyberangreb-kan-koste-trecifret-milliardbeloeb/artikel/3167992

- Opråb efter hackerangreb: Husk nu at opdatere dit antivirusprogram, Danmarks Radio, Per Bang Thomsen, May 2017. Available at: http://www.dr.dk/nyheder/indland/opraab-efter-hackerangreb-husk-nu-opdatere-dit-antivirusprogram
- UK hospitals hit with massive ransomware attack, The Verge, Russel Brandom, May 2017. Available at: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin
- Are Android Devices Really Easier to Hack?, Digital Trends, Simon Hill, May 2017. Available at: https://www.digitaltrends.com/mobile/are-android-devices-really-insecure-we-asked-some-experts/
- An Introduction to Behavioral Economics, Alain Samson, PhD, 2014. Available at: https://www.behavioraleconomics.com/introduction-to-be/
- Private er i stigende grad mål for IT-kriminelle, Danmarks Radio, Mads Allingstrup, January 2015. Available at: https://www.dr.dk/nyheder/viden/tech/private-er-i-stigende-grad-maal-it-kriminelle
- Spis æg med god samvittighed, Søndagsavisen, Trine Fisker, May 2016. Available at: https://www.sondagsavisen.dk/mad/madogsundhed/2016-03-23-spis-aeg-med-god-samvittighed/
- It-sikkerhed: Stigning I ransomware angreb er ude af kontrol, Version 2, Morten Egedal, February 2017. Available at: https://www.version2.dk/artikel/it-sikkerhed-stigning-ransomware-angreb-ude-kontrol-1073737
- WannaCry Ransomware Demonstrates The Value Of Better Security and Backups, Forbes, Tom Coughlin, May 2017. Available at: https://www.forbes.com/sites/tomcoughlin/2017/05/14/wannacry-ransomware-demonstrations-the-value-of-better-security-and-backups/#3d52085f70b8
- Se hvor stor risikoen for indbrud er i dit område, Politiken, Annemette Grundtvig, December 2016. Available at: http://politiken.dk/forbrugogliv/art5751112/Se-hvor-stor-risikoen-for-indbrud-er-i-dit-omr%C3%A5de
- Højsæson for alarmer: Vi sikrer vore huse som aldrig før, Danmarks Radio, Lars Von Magius, June 2014. Available at: https://www.dr.dk/nyheder/regionale/trekanten/hoejsaeson-alarmer-vi-sikrer-vore-huse-som-aldrig-foer
- Enduarance Test: Does antivirus software slow down PCs?, AV-test, Markus Selinger, April 2015. Available at: https://www.av-test.org/en/news/news-single-view/endurance-test-does-antivirus-software-slow-down-pcs/
- The Extended Mind Thesis, Oxford Bibliographies, Julian Kiverstein, Mirko Farina and Andy Clark, October 2015. Available at: http://www.oxfordbibliographies.com/view/document/obo-9780195396577/obo-9780195396577-0099.xml
- Tillidssamfundet Danmark, Børsen, Peter Holdt Christensen, Ph.D at Copenhagen Business School, October 2006. Available at: http://borsen.dk/nyheder/avisen/artikel/12/1830955/artikel.html
- Bad News: 80% of Students can't Tell the Difference Between Real and Fake News, ScienceAlert, Fiona MacDonald, December 2016. Available at: http://www.sciencealert.com/bad-news-study-finds-80-of-students-can-t-tell-the-difference-between-real-and-fake-news

Appendix 1 - Interview guide

Attention on it-security

- How do you see the attention of consumers, citizens and companies on it-security?
- Do you think the consumers, citizens and companies should do more?
- How do you see the attention of politicians on it-security?
- Do you think politicians should do more?
- Do you think the current division of responsibility between consumers, citizens and politicians is fair?

Digital and analog

- Do you think digital threats are conceived differently than physical ones, and that this makes it-security feel less important?
- Is the physical distance between the crime and the criminal making it less obvious to citizens and politicians that something needs to be done?
- Do you think we need to use different methods, than the ones we use now, in order to have more focus on digital crime?
- Do you think people perceive digital crime as being less prohibited than physical crime?

Behavioral patterns

- Do you think consumers, citizens and companies are being overconfident in the digital sphere?
- Do you think this is why relatively few have reported digital fraud compared to actual accounts of it?
- Are people jeopardizing their own it-security by saving money on it-protection such as antivirus?
- Do people take bigger chances in the digital world than in the physical one, even though the consequences are the same?
- Billions are being used on making homes secure, but people as hesitant to spend money on it-security, why do you think this is the case?
- Do you think that miscalculation or a lack of knowledge is affecting people into not taking digital fraud more seriously?
- Do you think people are considering the consequences of giving away information in trade of services such as Google, Facebook or Tinder? Especially when keeping in mind the increasing exploitation of digital information?
- Do you think people actively consider how they are paying for their digital services?
- Do emotions play a role if people fear digital threats less than physical ones?
- Could it be recommended to help citizens to choose correctly by framing it-security differently?