Biases in security risk management: Do security professionals follow prospect theory in their decisions?

de Wit, J.J.; Pieters, Wolter; Jansen, S.J.T.; van Gelder, P.H.A.J.M.

DOI
10.18757/jisss.2021.1.5700

Publication date
2021

Document Version
Final published version

Published in
Journal of Integrated Security and Safety Science

Citation (APA)
de Wit, J. J., Pieters, W., Jansen, S. J. T., & van Gelder, P. H. A. J. M. (2021). Biases in security risk management: Do security professionals follow prospect theory in their decisions? *Journal of Integrated Security and Safety Science*, *1*(1), 34-57. https://doi.org/10.18757/jisss.2021.1.5700

BIASES IN SECURITY RISK MANAGEMENT: DO SECURITY PROFESSIONALS FOLLOW PROSPECT THEORY IN THEIR DECISIONS?

Johan de Wit [a,b,*], Wolter Pieters [c], Sylvia Jansen [d], Pieter van Gelder [a]

a Safety and Security Science Section, Faculty of Technology, Policy and Management, Delft University of Technology, The Netherlands

b Siemens Smart Infrastructure, Siemens Nederland N.V.

c Behavioural Science Institute, Faculty of Social Sciences, Radboud University, The Netherlands

d Faculty of Architecture and the Built Environment, Delft University of Technology, The Netherlands

* Corresponding author, I.J.dewit@tudelft.nl

DOI: https://doi.org/10.18757/jisss.2021.1.5700

Keywords

Security
Decision making
Prospect theory
Risk management
Decision biases

Abstract

Security professionals play a decisive role in security risk decision making, with important implications for security in organisations and society. Because of this subjective input in security understanding possible biases in this process is paramount. In this paper, well known biases as observed and described in prospect theory are studied in individual security risk decision making by security professionals. To this end, we distributed a questionnaire among security professionals including both original dilemmas from prospect theory and dilemmas adapted to the context of incident prevention. It was hypothesised that security professionals dealing with risks and decision making under risk on an almost daily basis would or should be less vulnerable to decision biases involving risks, in particular when framed in terms of incident prevention. The results show that security professionals are vulnerable to decision biases at the same scale as lay people, but some biases are weaker when decision problems are framed in terms of security

as opposed to monetary gains and losses. Of the individual characteristics defining experience, only the general education level observably affects vulnerability for biases in security decision making in this study. A higher general education level leads to a significantly higher vulnerability to decision biases. By highlighting the vulnerability of security professionals to decision biases, this study contributes essential awareness and knowledge for improved decision making, for example by different representation of probabilities and uncertainty.

RESEARCH HIGHLIGHTS

- Decision making biases are, for the first time, identified in the professional security domain
- Comparisons between decision making by security professionals and lay-people are presented
- Psychological experiments are reformulated to reflect real life security decisions
- The results univocally show the vulnerability of security professionals to decision biases
- Unawareness of these biases might lead to less optimized security risk decisions

1. Introduction

Security professionals are confronted with the complex task of making decisions in security risk management processes . They are supposed to do this on a day to day basis with little specific (scientific) knowledge about the risks they are facing. They are expected to keep track of security risks threatening their domain of responsibility, act according to the risk appetite of the organisation, and balance security risk treatment (Wolf 2018; Butler 2002; Kayworth and Whitten 2010). The measures imposed to manage, or even mitigate, security risks need to be balanced between efficiency and effectiveness on one side and acceptance and invasiveness on the other. Due to the specific characteristics of security risks, their uncertainties, and the lack of (statistical) knowledge (Farahmand et al. 2003), this seems an impossible task. Still, in practice, tens of thousands security professionals globally take security decisions between different options day by day.

The main role of security professionals is to manage security risks. They need to identify, assess, evaluate and finally mitigate security risks. They are, or would expected to be, trained and educated to do this and build expertise over the years. Risks are generally seen as consisting of a kind of likelihood or probability that an associated impact occurs. Thus, dealing with risks in fact is dealing with uncertainties and probabilities, and balance them to potential benefits (Gordon and Loeb 2006; Kayworth and Whitten 2010; Butler 2002).

To fulfil this task, security professionals, at least in theory, are supposed to base their security risk decisions on risk management processes (Talbot and Jakeman 2011; Butler 2002; ISO/IEC 2016; NEN-ISO 2009; Button 2016; Forum 2018; NIST 2018). These risk management processes, by their nature, are a sequence of risk decisions as will be detailed in later sections. They urge the security professional to consider uncertainties and translate these in likelihood, in this paper further referred to as probabilities. As risk management is supposed to be an important and even guiding part of their work, security professionals can be expected to be familiar with decision making based on uncertainties and probabilities.

Previous well known studies into human decision making, like Prospect Theory (PT) (Kahneman et al. 1982; Kahneman and Tversky 1979) and Bounded Rationality (Gigerenzer, Todd, and ABC Research Group 1999; Simon 1982), have shown however, that humans are prone to 'misjudge' probabilities. They apply heuristics and show biases which make decision outcomes deviate from maximization theories like expected utility theory. This body of work unequivocally shows the use of heuristics and vulnerability for biases in decision making of humans. The experiments, however, are mainly performed in groups of lay people, often students. This might lead professionals, like security professionals, to believe these phenomena are less or not at all applicable to their judgement and decision making. Decision makers in general show a prevalence of overconfidence and often mistake their subjective sense of confidence for an indication of predictive validity (Kahneman 2021). It is therefore important to identify the use of heuristics and sensibility to biases in the actual professional community. If security professionals are vulnerable to these heuristics and biases, this could lead to less effective risk treatment or less efficient use of available resources. Or in other words they might decide to choose an less optimal risk mitigation alternative. Based on the presumed use of risk management processes, experience built over years, and trainings containing risk management, security professionals are hypothesised to be prepared for dealing with probabilities. At the same time, however, it can be expected that heuristics and biases play an important role. If this study makes these phenomena apparent in this community, as it does, security professionals cannot easily deny their influence in their day to day work.

This paper addresses the main research question: *Are security professionals vulnerable to decision making biases as presented in prospect theory?* Security risks and measures can be very diverse and are subject to individual subjective judgement.

To be able to study and compare decision making of individuals, the decision alternatives and their probability and impact are predefined. The original PT study focusses on decisions with two predefined options and thus is a suitable theory to investigate choice behaviour of security professionals. The decisions in PT are, however, defined in financial loss and gain. This might not be representing security decisions. Therefore, in the second part of this study, the decision alternatives are redefined in security risk mitigation or reduction. The expectation is that security professionals, by the nature of their work and expertise, and confronted with limited, predefined, and given probabilities, could be less biased than lay people. To answer the research question a survey amongst a convenience sample of security professionals is committed. The survey results will answer three sub questions:

1. To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using the original monetary gain and loss decisions?
2. To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using security decisions adapted from the original monetary ones?
3. To what extent do individual characteristics and security expertise, including age, experience, education and special security training, influence the vulnerability to decision making biases?

In section 2 of this paper risks are briefly described, and the specific characteristics of security risks are discussed. Section 3 contains a short introduction of a security management process and explains the role of decision making. The decision biases studied in this research are also clarified in this section. The methodology, survey methods and research boundaries are outlined in section 4. The results are presented and analysed in section 5. Finally, the paper ends with conclusions (section 6) and discussion and recommendations (section 7).

2. The subjectivity of security risk assessments

Decisions by security professionals are inherently based on subjective risk assessments. Risk is usually, and specifically in the context of (physical) security risk, considered as an unwanted event or an event with unwanted consequences which may or may not occur (Möller 2012; Hansson 2012; Rosa 1998). Risks in general, by their nature, contain a level of uncertainty. The uncertainty in the case of risks is originating from a lack of knowledge about the risk, the context, and/or the elements of risk itself: uncertainty about probabilities, vulnerabilities or consequences (Hansson 2012; Möller 2012; Vries 2017). Decision makers confronted with this uncertainty can decide to collect more information. A precondition for this is that the decision makers have time and resources to collect additional information. One could imagine many real-life situations where time and resources are (too) limited or the situation is (too) complex to collect sufficient risk information. About some risks there is simply no or no sufficient information available (Taleb 2007).

Security and security risks are risks and incidents resulting from malicious intent (Möller 2012; Talbot and Jakeman 2011). This study is limited to these risks. In security risks, the intent and persuasion of activities performed by malicious actors combined with the need to circumvent security measures leads to the need for unpredictable and often concealed behaviour (Hansson 2012). The virtually unlimited number of possible modus operandi and situational characteristics lead to a complex risk landscape, making prediction of probabilities and impact at least very difficult but most likely impossible (Möller 2012). Epistemic limitations like the rarity of some security incidents lead to a lack of historical data. Some security incidents are common (like for example intrusions) and historical data is available, but translating this data to probabilities for specific objects is given the situational, social-cultural and individual context of specific situations not reliable. This makes general historical data often not suitable for security risk

analysis for a specific case. In addition, security risk treatment takes many different shapes and forms. This large variety of possible treatment and actions offers security professionals a large basket of possible measures to choose from, ranging from physical fences to insurance policies.

The limited body of knowledge on security risk and security risk treatment leaves the security professionals with their own judgment and perception to guide their decisions. This judgment is based on the expertise of security professionals. Individual decision making is determined by personal/subjective characteristics and environmental/context/objective characteristics (Bandura 1986; Kämper 2000; Simon 1982; Smith, Shanteau, and Johnson 2004). Expertise is understood to be specialist knowledge acquired by education and experience (Bromme, Rambow, and Nückles 2001; Dingwall and Lewis 1983). In more detail expertise of an individual is defined by: experience, accreditation, peer-identification, reliability (between and within expert), factual knowledge and the availability of subject matter experts (Shanteau and Johnson 2004; Shanteau et al. 2003; Bueno de Mesquita 2010; Cooke 1991; Bontis 2001; Smith, Shanteau, and Johnson 2004). 'Risk assessment is inherently subjective and represents a blending of science and judgment with important psychological, social, cultural and political factors' (Slovic 1999). It is clear that (individual) perception of the decision maker about risks plays a crucial role in the assessment of risk, especially when there is a lack of information like in the case of security risk.

3. Risk management and decision making

To help professionals in their quest to identify, assess and treat risks in a systematic and transparent way risk management processes are designed (Koller 1999; Talbot and Jakeman 2011; NEN-ISO 2009; Purdy 2010; ISO/IEC 2016; Parkin 2000). Each stage of the process consists of a series of decisions (see Figure 1). Risk management can be considered as a process of successive decision making (Vries 2017). This paper will follow this view.

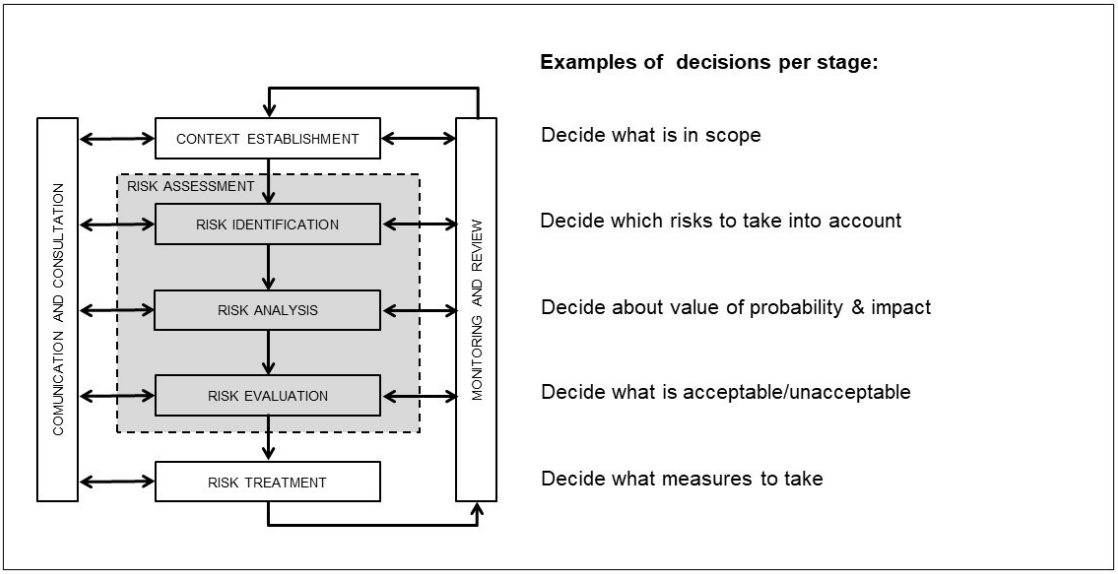

Figure 1. Risk management process according to ISO 31000 (NEN-ISO 2009) with examples of decisions per stage

In this paper a decision is defined as a choice leading to an outcome (Smith, Shanteau, and Johnson 2004; Jacob, Gaultney, and Salvendy 1986; Schick 1997). A decision situation is an actor facing a situation with a range of different decision alternatives. There are several assumptions about a decision making process (Doherty 2003; Collins and Ruefli 2012). First a decision process is expected to result in action or choice. Second a decision process requires the generation of a set of alternatives. Third these alternatives require a prediction of possible world states (or consequences). The consequences of a certain alternative have a degree of certainty of materializing. This degree of certainty is depending on the level of knowledge about the alternative and the consequences given a set of variables defined by specific circumstances and context (see Figure 2: first two stages of the decision making process). In the first stage, searching, alternatives are explored and defined according to search rules. In the following stage the search for alternatives is stopped according to stopping rules. At the stopping point the actor assumes there are enough alternatives available or the time, resources and cognitive capacity are too limited to search for or create more alternatives (Gigerenzer and Selten 2002; Golub 1997; Kämper 2000). Finally, a decision process requires the assessment of the stakeholders whether a world state (or set of consequences) is desired or not. The actor is supposed to be equipped with a set of preferences. These preferences will guide the actor's decisions. The consequences of the various alternatives will be evaluated against the actor's preferences. In this stage the decision is made which alternative to choose according to decision rules (Kämper 2000). The actor is expected to choose the alternative that serves his/her preferences best.

Decision making process				
Pre-decision	**Searching/ creating alternatives**	**Stop searching/ creating alternatives**	**Deciding**	**Post-decision**
- Awareness of problem/desire	- According to search rules	- According to stopping rules	- According to decision rules	- Consolidation (accountability, justification, dealing with dissonance,…)

Figure 2. Decision making process, inspired by Kämper (2000); Golub (1997); Gigerenzer and Selten (2002)

In the past substantial research is committed on the field of decision making under risk, starting with more normative theories like the Rational Choice Theory (RTC) the Expected Utility Theory (EUT) and the Subjective Expected Utility (SEU). These traditional decision concepts of maximization expect the actor to have knowledge of all the alternatives, all the possible consequences given specific circumstances, and context. This is also known as the Homo economicus model (Bazerman and Moore 1994). In practice the preconditions of these maximizing theories are practically impossible to meet. These theories are challenged in the previous century (Tversky and Kahneman 1975; Kahneman and Tversky 1979; Kahneman et al. 1982; Simon 1956; Simon 1982; Gigerenzer 2015; Gigerenzer and Selten 2002; Gigerenzer, Todd, and ABC Research Group 1999; Fischhoff 1982; Slovic 1999; Slovic 2000). The gap between the prescriptive decision models and outcomes of descriptive experiments were described and analysed (Keren and Teigen 2004;

Markman 2017). The reasons for deviations of optimization decisions theories were summarized in one of the main theories: prospect theory, PT (Kahneman and Tversky 1979; Kahneman 2012; Baron 2004). The PT, developed in the seventies of last century, is based on the results of various experiments in which the assessment of loss and gain, and the perception of probabilities by individuals is studied. These experiments showed various deviations from maximizing decision theories and inconsistencies in individual decision making. As these deviations and inconsistencies showed systematic tendencies over groups of respondents these are referred to as biases. The difference between the various decision theories like rational choice theory (RCT), expected utility theory (EUT), Prospect theory (PT) and Bounded rationality (BR), are not in the decision making process itself but can be found in the different searching, stopping and decision rules. As PT is based on experiments with pre-defined decision alternatives (usually alternative 'A' and 'B') applying searching and stopping rules is not a part of these experiments. PT and the experiments described in this paper are positioned in the 'deciding stage'.

PT presents decision heuristics and biases (Doherty 2003). The decision making heuristics and psychological biases explaining the behaviour of decision makers in PT are based on descriptive experiments. The known biases and heuristics from PT (Kahneman and Tversky 1979) are briefly described in this section. A bias is considered to show a systematic deviation from a norm. A heuristic on the other hand is considered a simplified method intended to cope with situations/problems within limited (human) processing capacity or 'rule of thumb' (Keren and Teigen 2004). Both biases and heuristics often are perceived as 'non rational' and error prone. Later research showed that the classification of some of the phenomena to be 'non-rational' can be rejected (van Erp 2017). In the experiments used in the original research the respondents are confronted with decisions with two predefined alternatives, 'A' and 'B', to choose from. In one of the experiments, for example, the respondents are asked to choose between alternative A: receive €4000 with a probability of 80%, or alternative B: receive €3000 with certainty (see decision 3, Table 1). An alternative (called prospect in PT) consists of outcome x_i with probability p_i. If the outcome of an alternative is certain (p_i=1) the outcome is denoted by (x). Loss is denoted by $-x_i$, a certain loss by (-x). The following phenomena from PT are part of this survey:

- The certainty effect. Actors generally tend to have a preference for certain outcomes (x) over risky outcomes even if the probability p_i is high and even if the weighed outcome of the risky outcome (p_i,x_i) exceeds the certain outcome (x), so even when (p_i,x_i) > (x) actors generally prefer (x). This effect is particularly relevant as it shows a deviation from optimizing the outcome. A smaller certain effect is preferred over a larger likely effect. When allocating resources this effect may lead to lower efficiency.
- The reflection effect. Actors generally prefer a risky negative outcome (p_i,$-x_i$) over a certain negative outcome (-x) even if the probability p_i is high and even if the weighed outcome of the risky outcome (p_i,$-x_i$) exceeds the certain outcome (-x), so even when (p_i,$-x_i$) < (-x), i.e. the weighed loss is higher, actors generally prefer (p_i,$-x_i$). Interestingly enough this effect shows completely reverse behaviour compared to the certainty effect when agents are confronted with loss. A lower but certain loss is avoided and a likely larger loss is accepted. As the negative impact of security risks usually is a kind of damage, disruption, or a decline in health, well-being or prosperity, it might be comparable with loss. In the security domain security risk management and reduction of a possible negative impact is considered the main goal of a security professional (Gill 2014). So, in this domain a level of professional risk aversion might be expected. The reflection effect, however, may lead to an opposite behaviour and increase risk taking.
- The isolation effect. In a decision containing several stages, actors generally tend to ignore stages that different alternatives have in common. In such a case actors usually focus

their decision on the last stage/decision only, which might lead to a suboptimal outcome. In a process of sequential decisions, like a risk management process, this effect shows a level of ignorance for a comprehensive view on a combination of decisions. The last decision of the sequence is dealt with in isolation ignoring previous ones. One of the leading elements in security risk management: layers of defence, is based on the implementation of multiple, independent, risk reduction measures. These subsequent risk reduction measures, *in combination*, should reduce the risk to an acceptable level. The isolation effect indicates that individuals are tempted to only take the last decision into account and ignoring the previous stages. This effect, when identified in behaviour of security professionals, could indicate that they take only the last decision or layer into account.

- Non-linear preferences (value function or probability distortion). In dealing with probabilities expectations are that the perception of percentages is linear. 'One percent is one percent'. Experiments show however that the perception of one percent when changing from 100% to 99% is different than the perception of one percent in changing from 21% to 20%. In the same way is the perception of changing from 100% to 25% (divide by 4) different from 80% to 20%. This leads to the observation that percentages, although objective and quantitative, can have a different perception of their 'value' and thus can be perceived in a more subjective and qualitative way. A specially interesting phenomenon in relation to security risks is the observation that small probabilities tend to be overrated as a result of non-linear preferences. As security risks often have a low probability of occurring this phenomenon might make decision makers overrate them.
- Insurance/lottery effect. Actors weigh alternatives not solely on the perceived probability pi but take desirability of the outcome of an alternative into account. If an outcome is 'very desirable' but has a small probability, this alternative might be preferred over an alternative with the same weighed value but with an outcome that is less desired. In combination with the reflection effect the weighing function directs decisions in the opposite direction if an alternative has a 'strong not desired outcome'. Both the desire to gamble, as a gain is at stake, and the willingness to buy insurance in the case of a possible loss are a result of this observed effect. Testing the vulnerability of security professionals for this effect might indicate their risk and insurance appetite.

As risks in general are usually weighed in terms of probability and impact these studied phenomena might have consequences for assessing risk and more specific security risks. The participants of the original experiments were mainly convenience samples of lay people and undergraduate students. The results, thus, might not reflect decision behaviour of experienced security professionals. Second, the original experiments consist of decisions with monetary gains and losses. This might not represent security risk decision making. In this paper, for the first time, to the best of our knowledge, the experiments are repeated specially targeted at security professionals and reformulated to better reflect security risk decision making. The latter is one of the main contributions of our study.

4. Methodology

In this study the experiments originating from PT are used to analyse decision making by individual security professionals. Security professionals are in this paper defined as individuals who are (partly) responsible for security risk management for a specific area of responsibility. In general this specific area of responsibility can take various forms like assets, locations, infrastructure, information, people, processes etc. The security professionals can be solely responsible or be part of decision making units. They can have a decisive or more advisory role. They can have a functional role in organisations like security officers, information security officers, risk managers or alike. They can also be consultants or part of

supplier organisations. What they have in common is that they play a decisive or influencing role in security risk management.

The survey is conducted among a broad selection of participants. The online survey is made available to participants of two security conferences in The Netherlands. The participants of the ASIS Security Management Conference are mainly physical security managers. The participants of the Information and IT Security Conference, on the other hand, are mainly IT and information security managers. Further survey sessions are done in the academic Safety and Security Science group of an University. This group is involved in research and evaluations of risk management processes, risk mitigation measures and risk prevention activities. A second survey group consisted of employees of a large security systems integrator. These individuals are involved in advising, planning, and implementing security systems and services in various markets. The sample and participants can be qualified as a convenience sample (N=69). The participants cover both the IT and physical security domain, have both advisory and responsible roles and finally cover all security processes from consultancy to implementation and services. Physical and IT security are to date separated domains with different threats, measures, and even different language and culture. The risk management processes, however, are similar (ISO/IEC 2016; ISO 2018; ASIS International 2015). Thus, although the content differs, the expected risk decision behaviour of security professionals in both domains is similar.

The basis for the survey are the decisions as used by Kahneman and Tversky in their original work (Kahneman and Tversky 1979). These are used to answer the first sub question: *To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using the original monetary gain and loss decisions?* The decisions in this part of the study are used in the exact same form and format as the original decisions. The amount of monetary gain and loss is kept the same as in the original decisions; the currency is set to Euros. The results of the security professionals are compared to the original results of lay people. This comparison, using identical decisions with a discrete outcome, is done using the Chi-square test of independence, for each decision separately. This part of the study compares the vulnerability of security professionals to lay people.

In the security domain, decisions take a form different from the original monetary decisions. To address this concern the experiments are reframed in risk mitigation characteristics, one of the main contributions of this study. For the second part of the survey the decisions are thus reformulated to better reflect security risk decision making and enable comparison with the results of the original experiments. Monetary gain and loss are replaced by 'a probability of achieving risk/incident mitigation' to answer the second sub question: *To what extent are security professionals vulnerable to decision making biases when the decisions mentioned above are adapted from monetary to security decisions?* These experiments are intended to reflect real life security decisions like: which control do I implement: control measure A with these specific characteristics or control measure B with another set of specific characteristics.

The participants are asked to respond to these reformulated decisions from the perspective that they are responsible for security. The respondents are informed in advance about the, for this study considered, leading security principle: minimization security risk is their main goal. As reduction of risk for 100% is not possible, 95% is considered as the maximum achievable result. As the effectiveness of security measures is not certain in itself the prospect is defined as an expected chance of achieving an expected percentage of reduction of incidents. The probability of a monetary gain in the original decisions is thus redefined as a probability of achieving a percentage of reduction of security incidents. A monetary loss is replaced by a number of security incidents as experiencing a security incident is considered to be felt like a loss. The probability of experiencing a monetary loss in the original decisions is redefined as a probability on experiencing a number of

security incidents. The ratio of the weighed expected outcome of the alternatives is kept similar and/or concordant between the two sets of decisions. For example: the respondents are asked to choose between alternative A; implement security measures with 80% probability of reducing the number of security incidents by 95%, or alternative B; implement security measures with 100% probability of reducing the number of security incidents by 70%.

The responses to this second part of the study are compared within the same group of security professionals applying the McNemar Change test for two related samples. This test examines whether or not the responses within the same sample group differ between the two occasions for similar decision problems. Two decisions, differing from the original ones are added in this second part of the survey. These decisions offer a third decision alternative 'C': the security measures will not be implemented. These decisions also contain a cost component (see decision 18 and 19 in Table 2). Adding those criteria and alternative might lead to different decision behaviour. It might indicate a role of cost criteria in security decision making. Further details are discussed in section 5.2.

In the third section of this study the influence of personal characteristics and several aspects of individual expertise are evaluated. The third sub question: *To what extent do individual characteristics and security expertise, which includes age, experience, education and special security training, influence the vulnerability to decision making biases?* is answered based on a third set of questions. For each respondent the number of decisions in which they follow the expected bias is calculated. Grouping the respondents based on the individual characteristics age, number of years professional experience, number of years in current position, education level, and security training, a group average of number of followed biases is calculated. These group averages are compared using statistical tests (Anova). Based on these results the influence of the different studied individual characteristics on vulnerability to decision biases under study can be identified.

In addition to the individual characteristics, two general organisational classifications are collected to get a grasp of the organisational context of the respondents. First the organisational sector of the respondents is asked: public sector or private sector. The other organisational question relates to the organisational size defined in the number of employees. These two questions are included to see if there is any indication of influence of the professional environment that would justify further research. These characteristics are analysed similar to the individual characteristics.

Participants are informed about the goal of the survey, understanding decision making in the security domain and testing decision making theory of Kahneman and Tversky. The participants are asked to respond to these reformulated decisions from the perspective that they are responsible for security. Their input is processed anonymously. The survey consists of 13 decisions in the original form, see Table 1, 11 decisions with reformulated security utility (see Table 2) and 8 general/personal questions on age, experience, education, trainings and organisational classification (see Table 3).

There are drawbacks on using hypothetical survey decisions. The validity and generalizability of the results remains questionable as in every laboratory setting. In the security domain with its human dynamics and malicious intent both the threats and the measures can be perceived differently by individual security decision makers. Setting up pre-defined alternatives with a given and specified probability and consequence, however, filters out individual perception and makes results comparable. Using monetary values representing consequences also introduces some constraint. A monetary value solely might not do justice to the various perceptions and values of consequences and thus make a decision less realistic (Schneider and Barnes 2003). The upside of using this simplification of reality is the univalent perception and comparability. The assumption is that the

participants have no special reason to disguise their true preferences.

5. Analysis and findings

The results are presented in the next three sections. In section 5.1 the results of the original research and lay respondents are compared to the results from the security professionals. Section 5.2 contains the results of the reformulated security decisions. The responses of the sample of security professionals on the original decisions are compared to the responses to the reformulated security decisions. Finally in section 5.3 the results of the security decisions are analysed based on individual and organisational characteristics of the respondents (age, experience, education, trainings, organisational classification, organisational size).

5.1 Analysis and findings part 1 comparing responses to original decisions

The decision problems in this part are presented to the respondents as shown in the left column of Table 1 and are labelled from 1 to 13. For example, for the first decision problem the respondent is presented with a choice between receiving €2400 for certain (alternative B) or a gamble with 33% chance to receive €2500, 66% chance to receive €2400 and 1% chance receiving €0 (alternative A). In the original study by Tversky and Kahneman 82% (n=59) of respondents chose the certain alternative. In our study, 80% of respondents (n=51) chose the certain alternative. The Chi^2 test for this decision was non-significant, indicating that the security professionals did not differ in their response to this question from the respondents in the study by Tversky and Kahneman. The column 'expected bias' indicates the alternative that in the original study was preferred by the majority of the respondents. This behaviour is explained as bias in the original paper. The biases and the consequences of these biases are discussed in more detail in this section.

The calculations for decisions 1 to 13 are shown in Table 1. H_0 cannot be rejected for all decisions except for the decisions 2, 10 and 12. For these decisions H_0 can be rejected ($p<0.05$), meaning that the responses from the group security professionals differ from those of the respondents in the original study (Kahneman and Tversky 1979). The responses of these exceptions are, however, concordant between the two groups (in both samples: decision 2: $x_A>x_B$, decision 10: $x_A<x_B$, decision 12: $x_A<x_B$). In other words: the tendency to follow the biases is present in both sample groups. After inspection of Table 1 it is clear that the security professionals have a tendency to follow the bias. However, for dilemmas 2, 10 and 12 they seem to do so to a smaller degree than the original respondents in the original study. For the other dilemmas no difference between the two respondent groups is observed, meaning that the security professionals follow the bias to about the same degree as the original respondents. The results of the individual decisions will be discussed in more detail and related to the biases in the remaining part of this section.

Certainty effect

The responses to decisions 1 and 3 clearly show a tendency to choose certainty over risk when there is a monetary gain at stake. Although in both cases the weighed outcome ($p_i.x_i$) is higher than the certain outcome the respondents choose certainty. They are willing to 'pay' to avoid uncertainty. In decision 1 the chance of receiving less than €2400 is only 1%, the chance of receiving €100 more is 33%. The 1% probability seems to be overrated by the majority of respondents. In decision 3 the chance of receiving less than €3000 is 20% while the chance of receiving €1000 more is even 80%. The lack of statistically significant differences in the responses to these dilemmas between the two respondent groups justifies the conclusion that the sample of security professionals seems to be as vulnerable to the 'certainty effect' as lay people.

Table 1. Chi-square calculation decisions 1-13

	Alternatives		Answers					Chi-square calculation		
			Security Professionals			Original results Kahneman & Tversky				
			%	N	Expected bias	%	N	X2	p-value	N
Decision 1	A	33% probability of receiving €2.500,= 66% probability of receiving €2.400,= 1% probability of receiving €0,=	20	13		18	13	0.11	0.74	136
	B	Receive €2.400,= with certainty	80	51	B	82	59			
Decision 2	A	33% probability of receiving €2.500,= 67% probability of receiving €0,=	53	34	A	83	60	14.49	**<0.05**	136
	B	34% probability of receiving €2.400,= 66% probability of receiving €0,=	47	30		17	12			
Decision 3	A	80% probability of receiving €4.000,=	25	17		20	19	0.50	0.48	164
	B	Receive €3.000,= with certainty	75	52	B	80	76			
Decision 4	A	20% probability of receiving €4.000,=	62	43	A	65	62	0.15	0.70	164
	B	25% probability of receiving €3.000,=	38	26		35	33			
Decision 5	A	45% probability of receiving €6.000,=	19	13		14	9	0.67	0.41	135
	B	90% probability of receiving €3.000,=	81	56	B	86	57			
Decision 6	A	1% probability of receiving €6.000,=	73	50	A	73	48	0.00	0.97	135
	B	2% probability of receiving €3.000,=	27	19		27	18			
Decision 7	A	0.1% probability of receiving €5.000,=	63	40	A	72	52	1.46	0.23	136
	B	Receive €5,= with certainty	37	24		28	20			
Decision 8	A	80% probability of losing €4.000,=	84	56	A	92	87	2.43	0.12	162
	B	Lose €3.000,= with certainty	16	11		8	8			
Decision 9	A	20% probability of losing €4.000,=	54	36		42	40	2.13	0.14	162
	B	25% probability of losing €3.000,=	46	31	B	58	55			
Decision 10	A	45% probability of losing €6.000,=	63	42	A	92	61	16.83	**<0.05**	133
	B	90% probability of losing €3.000,=	37	25		8	5			
Decision 11	A	1% probability of losing €6.000,=	27	18		30	20	0.19	0.66	133
	B	2% probability of losing €3.000,=	73	49	B	70	46			
Decision 12	A	0.1% probability of losing €5.000,=	32	20		17	12	4.22	**<0.05**	135
	B	Lose €5,= with certainty	68	43	B	83	60			
Decision 13		**First stage:**								
		75% losing, out of the game								
		25% winning, go to the second stage and choose option A or B								
		Second stage:								
	A	80% probability of receiving €4.000,=	17	11		22	31	0.55	0.46	204
	B	Receive €3.000,= with certainty	83	52	B	78	110			

Decision 2 is comparable to decision 1 (note that in decision 2 in both alternatives A and B, 66% of receiving €2400 is removed). Whereas these decisions are similar but formulated in a different way, similar choices would be expected on both decisions. Nevertheless, Kahneman and Tversky noticed in their research that 61% of their respondents changed from alternative B for decision 1 to alternative A for decision 2. In the case of the security professionals this percentage is 44%. So, although this percentage is somewhat less than the percentage reported by Tversky and Kahneman, it shows that almost half of the security professionals make a different decision when a sure gain is changed in a probable one. The majority of the security professionals violate the EUT for both decision 1 and 2.

The responses to decision 3 clearly show the certainty effect. The alternatives described at decision 4 are exactly ¼ of the alternatives at decision 3. However, respondents in both samples provide opposite responses to dilemmas 3 and 4. The analysis of the responses from the security professionals shows that 46.4% of the respondents changes from B at decision 3 to A at decision 4 . It seems that lowering the probabilities of a gain changes decision behaviour considerably. For this result, the security professionals do also not seem to behave differently from the original respondents.

Non-linear preferences (value function or probability distortion)

The influence of the reduction of probabilities by a factor four between decisions 3 and 4 show a stronger effect on the responses to alternative B (from 100% to 25%) compared to the responses to alternative A (from 80% to 20%). 29% of the respondents stick to their choice for alternative B at both decision 3 and 4. A significant number of 46% of them changes from B to A. Only 16% chooses A at both decisions and 9% shift from alternative A at decision 3 to alternative B at decision 4. The influence of probabilities is further tested with decisions 5 and 6. The given alternatives have exactly the same weighed outcome in both decisions. In both decisions the probabilities differ by a factor two. In decision 5 the probabilities are relatively high (45% and 90%). The respondents focus in this case on the probabilities and choose the alternative the highest probability. In decision 6 the probabilities are relatively low (1% and 2%). In this case the respondents seem to base their decision on the highest gain. 58% of the respondents from the group security professionals change from alternative B at decision 5 to alternative A at decision 6. Besides this, the security professionals and the lay people do not differ in their response to dilemmas 5 and 6. Thus, security professionals seem to be as vulnerable to the bias with regard to non-linear preference as lay people are.

Combining the results of decisions 3, 4, 5 and 6 lead to the observation that when the probabilities are relatively high and the consequence is a gain the security professionals (like lay people) base their choice on the probability (decision 3: 100% and, decision 5: 90%). When the probabilities are relatively low and the consequence is a gain the respondents seem to base their choice less on probability and more on the (desired) consequence. This is particularly interesting in the security domain where probabilities of an event occurring are relatively low. Based on these results decision behaviour of security professionals seems to shift between probabilities of 45% and 20% (probability > 45%: the majority chooses the highest probability, see decisions 3 and 5, probability < 20%: the majority chooses the preferred consequence, see decisions 4 and 6). The original results of lay people are almost identical and show similar behaviour.

Reflection effect

In their theory Kahneman and Tversky noticed opposite choices when instead of possible gains, possible losses were at stake. They labelled this the 'reflection effect'. Decision 8 is the opposite of decision 3, decision 9 the opposite of decision 4, decision 10 the opposite of decision 5 and decision 11 the opposite of decision 6. As shown in Table 1 it is highly likely that the group security

professionals is responding similar to lay people at decisions 8, 9 and 11. The responses to decision 10 are concordant between the two groups. The statistically significant difference between the respondents in the study by Kahneman and Tversky and the current study for decision problem 10 shows that the security professionals are somewhat less likely to make an entirely different decision for decision problem 10 compared to decision problem 5. This can also be seen for the coupled decision problems 3-8 and 4-9, although for these decision problems the difference between the two groups do not reach statistical significance. Nevertheless, it is safe to conclude that the security professionals in this sample are also vulnerable for the reflection effect. The responses of the security professionals to the decisions 8 and 9 also violate the EUT.

The decisions 5 and 10 consist of choices with the exact same weighed outcome. Respondents are asked to choose between probabilities of 45% vs. 90%. In case of a gain (decision 5) 82% of the respondents chooses the alternative with the 90% probability. The respondents show a preference for more certainty when there is a possible gain at stake. When the possible gain is changed in a possible loss at decision 10, 63% of the respondents choose the alternative with the 45% probability. In the case of a possible loss the reflection effect seems to guide the decisions of the majority of the security professionals.

In the decisions 6 and 11 the probabilities are relatively low: 1% and 2%. Both alternatives have the exact same weighed value. At decision 6 (gain) 73.1% of the respondents chooses for the lower probability (they seem to focus on the more desirable consequence). At decision 11, where a loss is at stake, exactly the same percentage of people choose the opposite alternative with the higher probability but with also the more desirable consequence (a lower loss).

Decision 11 can be considered as coming close to security risk decisions. Usually security risks have a 'low' perceived probability and when materializing introduce a consequence that can be considered a loss. The responses to decision 11 seem to indicate that the perceived negative consequence drives the decision rather than the (small) difference in probability.

Lottery and Insurance effect

When gains are at stake and probabilities are relatively low, choices focus on the weight of the gain, as already shown in the section on non-linear preferences (see decisions 4 and 6 in Table 1). When this heuristic is combined with the certainty effect the lottery effect can be clearly observed. In decision 7 a small probability with high gain is offered together with a certain gain. Note that the weighed outcome of both alternatives is equal. Two thirds of the security professionals choose to gamble instead of an equally weighed certain gain. In other words they are willing to give up a certain small monetary gain (premium) for the (very small) chance on a bigger gain. The percentage of security professionals that is willing to gamble is 9% lower than in the sample of lay persons, this is , however, not significant.

The opposite effect can be observed if the gains are replaced with loses (see decision 12 in Table 1). In this case a certain loss is clearly preferred over a small possibility of a bigger loss (again with the same weighed outcome). This pattern is labelled the 'insurance effect'. It is the willingness to accept the loss of a certain small amount to avoid a possible bigger loss. The difference between the two sample groups is in this case statistically significant. While in the original sample of lay persons 83% rather pays the certain premium to avoid a loss, in the sample of security professionals this percentage is 68%. These results seem to show that security professionals are less risk averse than lay persons at this decision. Although the majority of security professionals seem to be willing to pay the premium, almost 1 in three is willing to take the risk and would not choose 'insurance'.

Isolation effect

When people are confronted with situations consisting of a series of subsequent decisions they tend not to consider the overall expected outcome.

Instead they focus on the final decision. This phenomenon is labelled the isolation effect by Kahneman and Tversky. Based on the results of this survey it is safe to conclude that the group of security professionals is vulnerable to this effect.

Decision 13 is set up as a two stage decision. The first stage offers a 75% chance of receiving nothing and a 25% chance of entering the second stage. Respondents have no influence on this stage. In the second stage alternative A offers an 80% chance on receiving €4000 and alternative B of receiving €3000 with certainty. Notice that stage 2 is identical to decision 3. Calculating alternative A over the two stages leads to: x_A = 25% * 80% * €4000 ; this equals 20% * €4000. Calculating alternative B leads to x_B = 25% * 100% * €3000. Alternative B equals 25% * €3000. Notice the combined outcome of the alternative A and B over the two stages is identical to decision 4. Respondents who consider both stages are, therefore, expected to choose identically to their choice at decision 4. If the respondents only consider the second stage of decision 13 they would choose identically to decision 3. The response of the sample of security professionals to decision 13 clearly shows a strong preference for the latter. 83% of the respondents chooses alternative B at decision 13 compared to 75% at decision 3. The certainty effect is even stronger at the two-stage decision. Only 9.5% of the security professionals choose A at both decisions 13 and 4 which would show a consideration of both stages and would be the preferred outcome based on EUT. The responses of the sample of security professionals do not differ significantly from the responses of the original sample.

5.2 Analysis and findings part 2: comparing original decisions to security utility decisions

The decision problems in this part are presented to the respondents as shown in the left column of Table 2 and are labelled from 14 to 24. The alternatives at the decisions 14 to 24 are formulated with a security expected utility or prospect. For example, decision 16 is similar to decision 3 but the respondent is presented with a choice between B: reducing security incidents with 70% for certain (this replaced the original 'receiving €3000 for certain') or A: reducing security incidents with 95% (the maximum achievable outcome) with a probability of 80% (this replaced the original '80% probability of receiving €4000'). The majority of security professionals (75%) chose for certainty at decision 3 compared to 54% at decision 16. The responses of the security professionals to the original decisions and to the reformulated decisions are compared using the McNemar Change test for two related samples. The results of the different comparisons are shown in the fourth column of Table 2. For all but decisions 16, 22 and 23 no statistically significant change in response is observed. This implies that for the majority of the decisions changing the monetary gain and loss into security gain and loss has no significant effect on the decisions made by the respondents. The perception of the security professionals of a *monetary gain* seems to be comparable to a *reduction of security incidents* (at least both lead to the same decision behaviour).

Comparing the monetary decisions to the security decisions shows concordant responses except for the decisions 22 vs. 8 and 23 vs. 9. In these two exceptions the majority of the respondents choose the alternative with the best weighed outcome when the expected utility is expressed in number of incidents (decisions 22 and 23). At decisions 8 and 9, where the utility is expressed in a monetary loss, the majority of the respondents choose the alternative with the lowest certainty due to the reflection effect (aversion to certainty of loss). These alternatives have a lower weighed outcome. As described in more detail in the methodology section a *monetary loss* of the original experiments is replaced by *experiencing security incidents*. This is based on the assumption that a security incident would be perceived as a loss. The results as detailed above, however, show different decision behaviour leading to the observation that security professionals do not seem to perceive security incidents similar as (monetary) losses. Further research into this topic is needed to verify this observation.

The decisions 18 and 19 are added to the survey to test if adding costs would change decision behaviour. In these decisions also a third choice alternative is added: the security measures will not be implemented. The monetary price of the security measures, €100.000 is an arbitrary amount. It is defined based on practical operational experience in corporate and government environments and common order of magnitude of security investments. It is high enough to need serious consideration by a security professional. On the other hand it is not as high that it would not be considered at all. Decision 18 is identical to decision 16 and decision 17 is identical to decision 19 except for the third choice alternative.

The comparison of decision 16 vs. 18 shows that the majority of the respondents choose the same alternative and stick to their choice (67%), only 11 % chooses alternative C and decides not to implement the security measures.

The comparison of decision 17 vs. 19 shows a very different behaviour. 33% of the respondents stick to their choice while 59% chooses alternative C. It is clear that investing €100.000 is perceived justified by the vast majority (90%) of the respondents when security risks are reduced by 76% or 70% (the weighed outcome of decisions 16 and 18). When the risks are reduced by 18% or 19% (the weighed outcome of decisions 17 and 19) only 41% of the respondents is willing to invest this amount. These results show that security professionals weigh their investments against the perceived value they bring (in this case a probable reduction of security incidents). In search for the criteria which form the basis for security risk decisions it seems clear that the level of investments and risk reduction are related and are part of these criteria. Further research should be committed to define probable further criteria and their relationship.

5.3 Analysis and findings part 3: Influence of expertise, experience and age on security decision making

Security professionals are supposed to have expertise in their field to guide their decisions. In this survey the individual expertise is defined on some easily classifiable individual characteristics of the respondents. Accreditation and (supposed) factual knowledge are in this survey specified by education (general level and special security trainings). Experience is defined by professional position, number of years in this position, number of years professional experience and age. Table 3 shows the overall averages of the response to the reformulated security decisions 14-24 classified by the individual characteristics.

The results of the security professionals are also analysed against two general organisational classifications. First is the classification of the sectors 'public' or 'private' where the organisation of the security professionals is positioned in. The second organisational question relates to the organisational size defined in the number of employees (see Table 3).

To examine whether groups of respondents differ in their vulnerability to biases, based on the personal characteristics reported in Table 3, for each individual respondent number of decisions in which they follow the expected bias is calculated. Decision 18 and 19 are excluded from this average as they offer three options. Over the remaining nine decisions the respondents, on average, follow the expected bias at 5.98 out of 9 decisions (N=59). Based on the individual criteria relations between the individual averages and the variables age, total years professional experience, years in current position, educational level, and security trainings are investigated.

There is no statistically significant difference between the group means of the different age groups presented in Table 3, as determined by one-way Anova ($F(3,55) = 1.057$, $p = 0.375$). Also no statistically significant difference is determined between the different groups as categorized in the total years professional experience ($F(4,54) = 1.292$, $p = 0.285$) and the numbers of years in the current profession ($F(4,54) = 0.594$, $p = 0.669$). Respondents that indicate to have followed specific security training do not show a significantly different decision behaviour compared to those

without this training ($F(1,57) = 1.169$, $p = 0.284$). These four individual criteria do not seem to significantly influence vulnerability to decision biases.

Table 2. Comparing security decisions vs. monetary decisions, responses of sample group security professionals

			Answers									
		Alternatives	Security decisions			Monetary decisions			McNemar		Combined	
			%	N	Expected bias	Decision	%	N	p-value	N	Expected combined bias	Following combined bias %
Decision 14	A	33% probability of reducing security incidents with 95% 66% probability of reducing security incidents with 90% 1% probability of not reducing security incidents	37	22		1	20	13	0.08	59	B-B	49
	B	Certainly reduce security incidents with 90%	63	37	B		80	51				
Decision 15	A	33% probability of reducing security incidents with 95% 67% probability of not reducing security incidents	64	38	A	2	53	34	0.12	59	A-A	34
	B	34% probability of reducing security incidents with 90% 66% probability of not reducing security incidents	36	21			47	30				
Decision 16	A	80% probability of reducing security incidents with 95%	46	29		3	25	17	<0.05	63	B-B	44
	B	100% probability of reducing security incidents with 70%	54	34	B		75	52				
Decision 17	A	20% probability of reducing security incidents with 95%	78	49	A	4	62	43	0.05	63	A-A	57
	B	25% probability of reducing security incidents with 70%	22	14			38	26				
Decision 18		Implement security measures costing €100.000,= with:										
	A	80% probability of reducing security incidents with 95%	41	26								
	B	100% probability of reducing security incidents with 70%	48	30	B							
	C	These security measures will not be implemented	11	7								
Decision 19		Implement security measures costing €100.000,= with:										
	A	20% probability of reducing security incidents with 95%	25	16	A							
	B	25% probability of reducing security incidents with 70%	16	10								
	C	These security measures will not be implemented	59	37								
Decision 20	A	45% probability of reducing security incidents with 95%	29	18		5	19	13	0.25	63	B-B	56
	B	90% probability of reducing security incidents with 45%	71	45	B		81	56				
Decision 21	A	1% probability of reducing security incidents with 95%	73	46	A	6	73	50	1.00	63	A-A	56
	B	2% probability of reducing security incidents with 45%	27	17			28	19				
Decision 22		A situation in which there is:							<0.05	63	A-A	40
	A	80% probability of having 100 security incidents/year	43	27	A	8	84	56				
	B	75 security incidents/year with certainty	57	36			16	11				
Decision 23		A situation in which there is:							<0.05	63	B-B	35
	A	20% probability of having 100 security incidents/year	25	16		9	54	36				
	B	25% probability of having 75 security incidents/year	75	47	B		46	31				
Decision 24		A situation in which there is:							1.00	63	B-B	57
	A	1% probability of having 100 security incidents/year	25	16		11	27	18				
	B	2% probability of having 50 security incidents/year	75	47	B		73	49				

Table 3. Overall averages following expected bias differentiated over individual characteristics

Average following expected bias differentiated over individual characteristics (calculated over 9 dilemmas: 14, 15, 16, 17, 20, 21, 22, 23 and 24)	**Total sample:**	**Age**				**Total years professional experience**					**Years in current profession**		
		<30	31-40	41-50	50>	<5	6-10	11-15	16-20	20>	<5	6-10	10>
N	59	9	15	21	14	8	8	6	11	26	29	18	12
Overall average of respondents following the expected bias	**66.5%**	64%	70%	67%	62%	67%	66%	78%	70%	63%	68%	68%	62%
Overall average in number of dilemmas in which the expected bias is followed by individual respondents	**5.98**	5.8	6.5	6.0	5.6	6.0	5.9	7.0	6.3	5.7	6.1	6.1	5.6

	General education level			**Specific security training**		**Number of employees in organisation**				**Sectors**	
	Associate degree	Bachelor degree	Master degree & PhD	Yes	No	0-250	250-1000	1000-5000	>5000	Public	Private
N	8	27	24	17	42	10	7	19	23	16	43
Overall average of respondents following the expected bias	51%	69%	69%	70%	66%	71%	73%	66%	63%	70%	66%
Overall average in number of dilemmas in which the expected bias is followed	4.6	6.2	6.2	6.3	5.9	6.4	6.6	5.9	5.7	6.3	5.9

The analysis of the categories of education level, however, does show statistically significant differences. The higher the education level of the respondents, as categorized in Table 3 (for the analysis the group academic/Master and PhD are combined), the more the respondents follow the expected biases ($F(2,56) = 4.883$, $p = 0.011$). Especially the difference between respondents with an associate degree (following bias at 4.6 out of 9 dilemmas) and the other two categories (both following bias at 6.2 out of 9 dilemmas) is remarkable. Based on these results there can be concluded that higher general education seems to increase the vulnerability to follow the investigated decision biases. The limited sample size in this survey, however, makes the results less conclusive.

The organisational context as based on the size of the organisation in number of employees does not show a significant influence ($F(3,55) = 1.047$, $p = 0.379$). The organisational sector, differentiated in government or non-government also shows no significant effect ($F(1,57) = 0.786$, $p = 0.379$).

At the level of the individual respondents significant differences can be observed, however, these generate no significant pattern except for general education level.

6. Conclusions

The results of this study indicate that the expectation: 'security professionals are due to their position and experience less vulnerable to decision biases as described in Prospect Theory' needs to be rejected. Based on the analysed results in section 5.1 the vulnerability of security professionals to decision making biases using monetary gain and loss decisions can be observed. Based on the decisions 1-13 (see Table 1) it is highly likely that the group of security professionals is responding similarly to lay people. For 10 out of the 13 decisions the decisions of the two samples, the security professionals and the original sample of lay people, do not differ significantly. The responses are concordant in 12 out of the 13 decisions. The influence of *the certainty effect, the non-linear preferences, the reflection effect, the lottery and insurance effect and the isolation effect* on decision making by the majority of the sample of security professionals is clearly observed. This

vulnerability to decision biases revealed on average in 70% of the sample of security professionals.

The vast majority of security professionals seems to experience the same vulnerability to biases in judging probabilities as lay people. As their work consists of dealing with security risks, which contain a level of uncertainty often expressed in a kind of probability, it is questionable if they reach an optimal decision. Although the decisions 1-13 do not reflect security decisions, the general biases in judging probabilities are found to be applicable on decision making by security professionals. Their role in the security domain and their experience does not seem to provide a better judgment of probabilities and thus risks.

The results of the reformulated decisions 14-24 show that on average two out of three respondents (66%) follow the expected biases even if the decision options are reformulated into more security-related outcomes. The results of section 5.2 (see Table 2) show that the vulnerability to decision biases is also significant when the decisions concern security utility as defined in this study.

Seventeen decisions of the total survey contained options with a different weighed outcome (the product of probability and outcome). Two different decision patterns can be observed. Ten of these decisions consist of options with a probability difference of 1% or 5% between option A and B. At eight of these ten decisions, the respondents choose the option with the best outcome, not the lowest probability. They also ignore the best weighed outcome in six decisions. The two exceptions can be explained by the certainty effect which is a strong behaviour driver as also identified in PT (Kahneman and Tversky 1979).

At all of the 7 decisions with a different weighed outcome and a probability difference of 20% or 45%, the respondents choose the option with best probability (which led to the worst weighed outcome at six of the decisions and violates maximizing theories). This leads to the following observation: if the probability difference is relatively small (in this survey 1% or 5%) respondents choose the option with the best outcome and they seem to ignore the difference in probability. If the probability difference is relatively large (in this survey 20% or 45%) they seem to base their decision solely on this and ignore the (weighed) outcome. This observation further expands the known non-linear preference effect or probability distortion.

Decisions between options with low probabilities

As security risks normally have a rather low probability of occurring it is interesting to pay special attention to the decisions 6, 11, 21 and 24 (see Table 4).

At all these decisions the options have a relatively low probability and the weighed outcome is equal (decision 21 almost equal). At all of the four decisions the majority of the respondents seem to base their choice on the desired outcome rather than the desired probability. They make identical choices in both the monetary as the security decisions. As the absolute difference is only 1% the previous observation seems to affect these decisions. The probabilities in these decisions however differ substantially when compared by each other (by a factor two). Risk is defined as a combination of probability (chance of materializing of the risk) and outcome (the expected consequences when a risk is materializing). So even if the respondents could decide to reduce the probability by a factor two (1% vs 2%) the majority choose not to.

Based on this observation it can be stated that in dealing with low probability risks the probability is ignored by decision makers. Decision options are solely judged on their perceived outcome. For the security practice this could mean that less effort could be put in investigating the probability of security risks (as they usually have a low probability of occurring). Further, lowering the probability of a risk is considered to be a preventive measure (it is less likely that the risk will materialize). The observation that for low probability risks the probability is ignored by

security professionals could, therefore, be interpreted as no or less focus on prevention. Their focus might be on reducing the impact or consequence solely. Theoretically these results indicate that the majority of the security professionals taking part in this survey seem to be less focussed on preventive measures (leading to lower probability).

Table 4. Responses of security professionals on decisions 6, 11, 21 and 24

	Alternatives		Answers		
			Security Professionals		Expected bias
			%	N	
Decision 6	A	1% probability of receiving €6.000,=	73	50	A
	B	2% probability of receiving €3.000,=	27	19	
Decision 11	A	1% probability of losing €6.000,=	27	18	
	B	2% probability of losing €3.000,=	73	49	B
Decision 21	A	1% probability of reducing security incidents with 95%	73	46	A
	B	2% probability of reducing security incidents with 45%	27	17	
Decision 24		A situation in which there is:			
	A	1% probability of having 100 security incidents/year	25	16	
	B	2% probability of having 50 security incidents/year	75	47	B

Influence of costs on security decision making

Decision 18 and 19 (see Table 2) offer a third choice option C: the security measures will not be implemented. There is also an arbitrary cost component added reflecting the costs associated with implementing the security measures. The options A and B at decision 18 are identical to these options at decision 16. Comparing the response shows that 67 % of the respondents choose alike on both decisions. Only 11% decides not to implement the security measures. The reaction to decision 19 shows a different behaviour. The options A and B at decision 19 are identical to these options at decision 17. Comparing these responses shows that in this case 33% chooses alike and 59% chooses option C. Based on these results it is safe to conclude that costs play a role in decision making of the respondents. In decision 18 89% of the respondents is willing to pay the premium of €100.000 to reduce risks with a probability of 80% or 100%. In decision 19 only 41% of the respondents is willing to pay the same premium for reducing risks with a probability of 20% or 25%. This difference indicates that the willingness to invest in security measures is related to the expected benefits. Based on the data resulting from just these two decisions no detailed conclusions can be drawn about this balance between costs and benefits. It is however safe to conclude that this relation exists. Further research might be committed to further specify this relation.

Important to note is that in decisions 18 and 19 no limitations on investments are imposed. It is therefore remarkable that a part of the respondents seems to be reluctant to invest in risk reduction even without budget restrictions.

Insurance effect

Decision 12 tests the insurance effect (see Table 1). Choosing between a small premium and a small probability on a relatively substantial loss is offered to the respondents. In the original research of Kahneman and Tversky 83% of the respondents chooses the premium over the risk. The security professionals show a significant different behaviour, 68% is willing to pay the premium. As security professionals are supposed to mitigate security risk they might be expected to be risk-averse. The results however show a significantly

higher percentage of them willing to take the risk compared to the original group of lay people.

The influence of expertise

Overall the respondents follow the expected bias in 6 of the 9 security decisions (decisions 14-24 except 18 and 19). Comparing the group means of the differentiated groups in age, number of years professional experience, number of years in current position, and conducted security trainings, show no significant difference. These variables do not influence the vulnerability for decision biases under study. For the security practice this seems to indicate that more experience and security knowledge as defined by these four variables does not lead to more optimized decisions.

A significant difference however is identified comparing the group means when the respondents are differentiated to education level. The results show a significant increase of vulnerability with a higher level of education. As no further detailed individual information is collected in this study no clear cause for this can be formulated. It is, however, an interesting finding which might inspire further research.

7. Discussion and recommendations

Because of the set-up of the present research, it cannot account for the full complexity of the tasks of security professionals. Because of the focus on prospect theory and associated biases, the present study highlights only one particular aspect of security decision-making. After participating in the survey several respondents reacted 'this is not the way decisions are made'. They indicated that, due to time pressures, incomplete information, and limited resource capacity, they follow different decision routines. Some of them seem to rely more on prior experience to guide their decision in a faster, more intuitive fashion. The results as presented in this paper, however, do not reveal influence of experience on the vulnerability for decision biases. This contradiction can be explained by the assumed decision process the decision maker follows. In this study the respondents are confronted with two predefined alternatives which might not comply to their real life decision making.

As already mentioned in the methodology section there are drawbacks on using hypothetical survey decisions. The validity and generalizability of the results remains questionable as a laboratory setting reflects only a selected part of reality. Due to the complexity of the security risk landscape, the virtually unlimited number of possible modus operandi, and the variation in situational, social-cultural and individual context, experiments need to simplify reality. The experiments in this study do not reflect an entire security risk assessment, they merely limit their scope to a choice between two mitigation options which in a real-life situation represents only a limited part of a risk assessment. However, we believe that PT can be made more realistic in a professional context by varying the types of questions asked. A key methodological innovation thus lies in de adaptation of generic PT dilemmas to a profession-specific context, in this case security incidents and associated probabilities.

Recommendations

Despite its importance in decision-making, the professionals in the security risk domain are largely unaware of psychological phenomena. It seems this knowledge is not included in the curricula of security professionals which in itself is an interesting observation of this study. As many decision makers, in general, show prevalence of over-confidence they might perceive their own judgement superior and believe they are not susceptible to biases. By replicating PT experiments in the actual professional domain, and adapting them to a security-specific context, the professionals acting in this domain cannot easily ignore the results and perceive their decision making superior to other humans. This awareness might be even the biggest contribution of this study to the security risk domain.

With respect to the overall research question, it is highly likely that security professionals are, in majority, vulnerable to decision making biases as presented in prospect theory. The results show

that they are as vulnerable to the investigated biases as lay people, which was not expected. This will influence security risk decision making and thus a security management process. Biases might lead professionals to less optimized security risk decisions which, in turn, might influence security in organisations and society. The results of this study can raise awareness for the identified biases. The logical subsequent step would be to take these biases into account and, if considered needed, take anti-biasing countermeasures. Other fields of research already identified these ranging from a different representation of probabilities and uncertainty (Gigerenzer 2015; Kurz, Gigerenzer, and Hoffrage 1998; Payne and Bettman 2001) to changing decision making processes (Stafford, Holroyd, and Scaife 2018; Trönnberg and Hemlin 2019; Simutis 2003; Daftary-Kapur, Dumas, and Penrod 2010). Many of these countermeasures are context related and thus the applicability for security risk decision making should be evaluated on a case by case basis. These tools can improve human security risk decision making and in turn improve our security.

References

ASIS International. 2015. "*Risk Assessment, ANSI/ASIS/RIMS RA.1-2015*." In. Alexandria: ASIS International.

Bandura, Albert. 1986. *Social foundations of thought and action: A social cognitive theory*: Englewood Cliffs, NJ, US: Prentice-Hall, Inc.

Baron, Jonathan. 2004. *Normative models of judgment and decision making*, Blackwell handbook of judgment and decision making: Wiley Online Library.

Bazerman, Max H, and Don A Moore. 1994. *Judgment in managerial decision making*: Wiley New York.

Bontis, Nick. 2001. "Assessing knowledge assets: a review of the models used to measure intellectual capital." *International journal of management reviews* 3 (1):41-60.

Bromme, Rainer, Riklef Rambow, and Matthias Nückles. 2001. "Expertise and estimating what other people know: The influence of professional experience and type of knowledge." *Journal of Experimental Psychology: Applied* 7 (4):317.

Bueno de Mesquita, Bruce. 2010. "JUDGING JUDGMENT." *Critical Review* 22 (4):355-88. doi: 10.1080/08913811.2010.541686.

Butler, Shawn A. 2002. *Security attribute evaluation method: a cost-benefit approach*. Paper presented at the Proceedings of the 24th international conference on Software engineering.

Button, Mark. 2016. *Security officers and policing: powers, culture and control in the governance of private space*: Routledge.

Collins, James M, and Timothy W Ruefli. 2012. *Strategic risk: a state-defined approach*: Springer Science & Business Media.

Cooke, R.M. 1991. *Experts in uncertainty.* New York: Oxford University Press.

Daftary-Kapur, Tarika, Rafaele Dumas, and Steven D Penrod. 2010. "Jury decision-making biases and methods to counter them." *Legal and Criminological Psychology* 15 (1):133-54.

De Vries, Jennie. 2017. "*What drives cybersecurity investment?*" (Master thesis), TU Delft.

Dingwall, Robert, and Philip Simon Coleman Lewis. 1983. *The sociology of the professions: Lawyers, doctors and others*: Macmillan; St Martin's Press.

Doherty, Michael E. 2003. *Optimists, pessimists, and realists, Emerging Perspectives on Judgement and Decision Research*. Cambridge: Cambridge University Press.

Farahmand, Fariborz, Shamkant B Navathe, Philip H Enslow, and Gunter P Sharp. 2003. *Managing vulnerabilities of information systems to security incidents*. Paper presented at the Proceedings of the

5th international conference on Electronic commerce.

Fischhoff, Baruch. 1982. "*Debiasing'in Judgment under uncertainty: heuristics and biases*. Daniel Kahneman, Paul A. Slovic, and Amos Tversky (eds.), 422-444." In.: New York: Cambridge University Press.

Forum, Information Security. 2018. "*Standard of Good Practice.*" In. Surrey: Information Security Forum.

Gigerenzer, Gerd. 2015. *Risk savvy: How to make good decisions*: Penguin.

Gigerenzer, Gerd, and Reinhard Selten. 2002. *Bounded rationality: The adaptive toolbox*: MIT press.

Gigerenzer, Gerd, Peter M Todd, and the ABC Research Group. 1999. *Simple heuristics that make us smart*: Oxford University Press.

Gill, Martin L. 2014. *The handbook of security*: Springer.

Golub, Andrew Lang. 1997. *Decision analysis: an integrated approach*: Wiley.

Gordon, Lawrence A, and Martin P Loeb. 2006. "INFORMATION SECURITY EXPENDITURES." *Communications of the ACM* 49 (1):121.

Hansson, Sven Ove. 2012. "*A Panorama of the Philosophy of Risk.*" In Handbook of risk theory, 27-54. Springer.

ISO. 2018. "*ISO 31000 Risk management - guidelines.*" In. Geneva: International Organization for Standardization.

ISO/IEC. 2016. "*ISO/IEC 27000 International standard Information Technology Security techniques.*" In. Geneva: ISO.

Jacob, Varghese S, Larry D Gaultney, and Gavriel Salvendy. 1986. "Strategies and biases in human decision-making and their implications for expert systems." *Behaviour & Information Technology* 5 (2):119-40.

Kahneman, Daniel, Sibony, Olivier., Sunstein, Cass R, 2021. *Noise, a Flaw in Human Judgment*. London: William Collins.

Kahneman, Daniel. 2012. *Ons feilbare denken: thinking, fast and slow*: Business Contact.

Kahneman, Daniel, Paul Slovic, Amos Tversky, and et al. 1982. *Judgment under uncertainty: Heuristics and biases*. Edited by Daniel Kahneman. Cambridge: Cambride University Press.

Kahneman, Daniel, and Amos Tversky. 1979. "Prospect theory: An analysis of decision under risk." *Econometrica: Journal of the econometric society*: 263-91.

Kämper, Eckard. 2000. *Decision Making Under Risk in Organisations: The Case of German Waste Management*: Ashgate Pub Ltd.

Kayworth, Tim, and Dwayne Whitten. 2010. "Effective information security requires a balance of social and technology factors." *MIS Quarterly executive* 9 (3):2012-52.

Keren, Gideon, and Karl H Teigen. 2004. "*Yet another look at the heuristics and biases approach.*" Blackwell handbook of judgment and decision making:89-109.

Koller, Glenn Robert. 1999. *The Practical Guide to Risk Assessment and Decision Making*: CRC Press.

Kurz, Elke, Gerd Gigerenzer, and Ulrich Hoffrage. 1998. "*Representations of uncertainty and change: Three case studies with experts*." In.: Sonderforschungsbereich 504, Universität Mannheim & Sonderforschungsbereich 504, University of Mannheim.

Markman, Arthur B. 2017. "Combining the Strengths of Naturalistic and Laboratory Decision-Making Research to Create Integrative Theories of Choice." *Journal of Applied Research in Memory and Cognition*.

Möller, Niklas. 2012. "*The concepts of risk and safety*." In Handbook of Risk Theory: Epistemology,

Decision Theory, Ethics, and Social Implications of Risk, 55-85. Springer.

NEN-ISO. 2009. "*NEN/ISO 31000 (nl) Risicomanagement-Principes en richtlijnen*." In. Delft: NEN.

NIST, National Institute of Standards and Technology. 2018. "*Framework for Improving Critical Infrastructure Cybersecurity*." In. Gaithersburg.

Parkin, James. 2000. *Engineering judgement and risk*. London: Thomas Telford Publishing.

Payne, JW, and JR Bettman. 2001. "*Preferential choice and adaptive strategy use*". In 'Bounded Rationality: the Adaptive Toolbox'. (Eds G Gigerenzer, R Selten) pp. 123–145." In.: Oxford University Press: New York.

Purdy, Grant. 2010. "ISO 31000: 2009—setting a new standard for risk management." *Risk Analysis* 30 (6):881-6.

Rosa, Eugene A. 1998. "Metatheoretical foundations for post-normal risk." *Journal of Risk Research* 1 (1):15-44.

Schick, Frederic. 1997. *Making choices: A recasting of decision theory*. Cambridge: Cambridge University Press.

Shanteau, James, and Paul Johnson. 2004. *Psychological investigations of competence in decision making*: Cambridge University Press.

Shanteau, James, David J Weiss, Rickey P Thomas, Julia Pounds, and Bluemont Hall. 2003. "How can you tell if someone is an expert? Empirical assessment of expertise." *Emerging perspectives on judgment and decision research*:620-41.

Simon, Herbert A. 1956. "Rational choice and the structure of the environment." *Psychological review* 63 (2):129.

Simon, Herbert Alexander. 1982. *Models of bounded rationality: Empirically grounded economic reason*. Vol. 3: MIT press.Simutis , Z.M. 2003. "Program in Basic Research 2002-2003." In. Fort Belvoir: US Army Research Institute.

Slovic, Paul. 1999. "Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield." *Risk Analysis* 19 (4):689-701.

Slovic, Paul Ed. 2000. *The perception of risk*: Earthscan publications.

Smith, Kip, James Shanteau, and Paul Johnson. 2004. *Psychological investigations of competence in decision making*: Cambridge University Press.

Stafford, Tom, Jules Holroyd, and Robin Scaife. 2018. "*Confronting bias in judging: A framework for addressing psychological biases in decision making*."

Talbot, Julian, and Miles Jakeman. 2011. *Security risk management body of knowledge*. Vol. 69: John Wiley & Sons.

Taleb, Nassim Nicholas. 2007. *The black swan: the impact of the highly improbable*. New York: Random House.

Trönnberg, Carl-Christian, and Sven Hemlin. 2019. "*Challenging investment decision-making in pension funds*." Qualitative Research in Financial Markets.

Tversky, Amos, and Daniel Kahneman. 1975. "*Judgment under uncertainty: Heuristics and biases.*" In Utility, probability, and human decision making, 141-62. Springer.

van Erp, Noel. 2017. "*A Bayesian framework for risk perception*." (Doctoral dissertation) Delft University of Technology.

Wolf. 2018. "An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication." *Behaviour and Information Technology* 37 (4):320-34.