

Risk Perception and Attitude in Information Security Decision-making

Konstantinos Mersinas

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

Information Security Group
School of Mathematics and Information Security
Royal Holloway, University of London
2016

Dedicated to my parents, Charilaos and Alikí,
to whom I not only owe my ζῆν (being),
but also my εὖ ζῆν (well being);
and to my wife, Maria,
for the inexhaustible support.

Declaration

These doctoral studies were conducted under the supervision of Prof. Keith M. Martin, Prof. Andrew Seltzer and Dr. Bjoern Hartig.

The work presented in this thesis is the result of original research carried out by myself, in collaboration with others, whilst enrolled in the Department of Information Security as a candidate for the degree of Doctor of Philosophy. This work has not been submitted for any other degree or award in any other university or educational establishment.

I, Konstantinos Mersinas, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Konstantinos Mersinas
December, 2016

Abstract

In an age in which humanity produces increasingly more data, information security is of critical importance. Risk, ambiguity and uncertainty are inherent features of information security, as potential threats can be known, imperfectly known or unknown.

Information security professionals have to assess risk and consequently decide on protective and corrective measures for treating this risk. We investigate whether professionals make such decisions optimally, in an objective way.

In order to do so, we conduct online experiments and surveys measuring perception and attitudes of security professionals towards risk. Participants are asked to state their willingness to pay (WTP) to avoid a series of losses-only lotteries, make choices between such lotteries and state their preferences over risk treatment actions. We examine professionals' behaviour in these lotteries as well as in security scenarios and conclude that security professionals do not minimise expected losses and cannot be considered as rational decision-makers.

We also contrast professionals' behaviour to that of a sample of university students and show that their preferences are measurably different in several respects. Both samples are found to be susceptible to inconsistencies between WTP and choice decisions. Risk attitude of participants is found to depend on the probability level of potential losses.

We devise a mechanism to elicit professionals' preferences between security and operability and find that the nature of their employment influences these preferences. Our findings suggest that security professionals are risk and ambiguity averse and are susceptible to framing effects when assessing and treating risk. Distinct preferences over risk treatment actions are also detected.

We interview renowned experts from the industry and academia about the implications of these findings. We conclude that these factors, being usually overlooked in risk assessment and treatment methodologies, need to be taken into consideration for the development of objective and unbiased risk management. Finally, we discuss implications and recommend approaches for de-biasing decision-making.

Acknowledgements

I would like to thank the three supervisors of this thesis, Keith, Andy and Bjoern. They all agreed to assist in this endeavour, by forming a multi-disciplinary group, and providing the expertise necessary in order to bridge information security and economics. They have all been very open-minded and I feel fortunate for our collaboration, especially at a time for my PhD research in which “winds were not fair” and “seas were not following”.

I would also like to thank Dr Colin Walter, for giving me the initial opportunity to undertake this research.

Thanks also to the ASECOLab crew: Bertfried, Alexandre, Christian, Muzamel and Liuxuan. Great team!

Finally, I thank my family for all their support throughout the years.

Contents

1	Introduction	18
1.1	Motivation	18
1.2	Overview of Methodology	22
1.3	Organisation of the Thesis	23
2	Background	25
2.1	Information Security	25
2.1.1	The Importance of Information Security	25
2.1.2	The Information Security Profession	26
2.1.3	Behaviour and Decisions in Information Security	31
2.1.4	Behavioural and Economic Approaches to Information Security	37
2.2	Economics and Behaviour	38
2.2.1	Decision-making Models of Risk Behaviour	40
2.2.2	Modelling Investment Decisions	56
2.3	Summary	60
3	Experiment 1: Decision-making under Risk and Ambiguity	61
3.1	Approach and Background	62
3.2	Methodology	63
3.2.1	Research Hypotheses	63
3.2.2	Experimental Procedure	64
3.2.3	Experiment Design	67
3.3	Analysis and Findings	74
3.3.1	Risk and Ambiguity Aversion	74
3.3.2	Worst-case Thinking	81

CONTENTS

3.3.3	Other-evaluation	88
3.3.4	Security - Operability Trade-off	89
3.3.5	Survey Analysis	93
3.4	Discussion	95
3.5	Summary	98
4	Experiment 2: Decision-making in Risk Treatment	99
4.1	Approach and Background	100
4.2	Methodology	102
4.2.1	Research Hypotheses	102
4.2.2	Experimental Procedure	103
4.2.3	Experiment Design	104
4.3	Analysis and Findings	106
4.3.1	Preferences over Risk Treatment Actions	107
4.3.2	Preferences between Probabilities and Outcomes	110
4.3.3	Framing of Decisions as Gains or Losses	112
4.3.4	Four-fold Pattern of Risk Attitude	121
4.4	Discussion	124
4.5	Summary	127
5	Implications	128
5.1	Summary of Findings	129
5.2	Supplementary Survey	130
5.3	Survey Findings	130
5.4	Semi-structured Interviews	139
5.4.1	Interview with David Brewer	139
5.4.2	Interview with Paul Dorey	142
5.4.3	Interview with Bruce Schneier	145
5.5	Discussion on Implications	146
5.5.1	Risk Aversion and Ambiguity Aversion	146
5.5.2	Performance of Professionals and Students	148
5.5.3	Professional Roles	149

CONTENTS

5.5.4	Proactive vs Reactive Security	150
5.5.5	Framing	151
5.5.6	Perception	152
5.5.7	Communication	154
5.5.8	De-biasing Decisions	155
5.5.9	Discussion on Recommendations	156
5.5.10	Summary	158
6	Conclusion	159
6.1	Key Research Findings	160
6.2	Future Research	161
A	Appendices	163
A.1	Appendix: Experiment 1	163
A.1.1	Experiment Design	163
A.1.2	H1 Instrument	163
A.1.3	Lottery Comparisons	164
A.1.4	H2 Willingness-to-pay Lotteries	165
A.1.5	Survey Questions	167
A.1.6	Experiment 1 Indicative Screenshots	169
A.1.7	Qualtrics Javascript Code	175
A.1.8	Experiment Analysis	185
A.1.9	Data Cleaning	185
A.1.10	Outliers	186
A.1.11	Controlling for Order Effects	187
A.1.12	Mathematica Code	189
A.1.13	SPSS Syntax Code	201
A.1.14	Linear Models Regression Specifications	232
A.1.15	Definitions	233
A.2	Appendix: Experiment 2	234
A.2.1	Experiment Design	234
A.2.2	Experiment 2 Indicative Screenshots	242
A.2.3	Definitions	251

CONTENTS

A.2.4	Qualtrics Javascript Code	252
A.2.5	Experiment Analysis	253
A.2.6	SPSS Syntax Code	253
A.3	Appendix: Modelling Investment Decisions	274
A.4	Appendix: Supplementary Survey	275
	Bibliography	280

List of Figures

2.1	Prospect theory’s hypothetical value function.	46
2.2	Risk attitude for gains: ratio c/x by the probability of gain.	47
2.3	Risk attitude for losses: ratio c/x by the probability of loss.	47
2.4	Indifference curves in the “Machina Ttriangle”	50
2.5	Iso-expected lines and indifference curves	50
2.6	Investment for achieving a more preferable state	51
2.7	Indifference curves for the domain of gains (left) and losses (right)	51
2.8	Values of salience function $\sigma(x, y) = \frac{ x-y }{ x + y }$, for $x \in (-1000, 0)$ and $y \in (-1000, 0)$	53
2.9	Levels of uncertainty.	56
3.1	Display Logic diagram for Hypothesis 4.	74
3.2	Mean risk-averse (positive) and risk-taking (negative) WTP of Students and Professionals per lottery. Bars represent participants’ mean WTP minus the EV of each of the 12 lotteries.	75
3.3	Interaction of <i>Pro or Student</i> and H_{19} with <i>General Risk</i> as moderator	77
3.4	Pairwise comparison of Group A lotteries for Students	80
3.5	Pairwise comparison of Group A lotteries for Professionals	80
3.6	Pairwise comparison of Group B lotteries for Students	80
3.7	Pairwise comparison of Group B lotteries for Professionals	80
3.8	Pairwise comparison of Group C lotteries for Professionals	81
3.9	L_9 or L_{10} : values of sum 3.9 for $L_9 \succ L_{10}$, $\delta \in (0, 1]$ (Students: 50%, Professionals: 59%)	86
3.10	L_{10} or L_{11} : values of sum 3.9 for $L_{10} \succ L_{11}$, $\delta \in (0, 1]$ (Students: 60%, Professionals: 53%)	86
3.11	L_8 or L_6 : values of sum 3.9 for $L_8 \succ L_6$, $\delta \in (0, 1]$ (Students: 48%, Professionals: 36%)	87

LIST OF FIGURES

3.12	L_6 or L_7 : values of sum 3.9 for $L_6 \succ L_7$, $\delta \in (0, 1]$ (Students: 60%, Professionals: 61%)	87
3.13	L_4 or L_{12} : values of sum 3.9 for $L_4 \succ L_{12}$, $\delta \in (0, 1]$ (Students: 52%, Professionals: 54%)	88
3.14	Security switching points ($Sec(x\%), Ops(10\%)$)	91
3.15	Operability switching points ($Sec(10\%), Ops(x\%)$)	91
3.16	Loss Aversion in Security ($Sec(-x + y\%), Ops(10\%)$)	91
3.17	Loss Aversion in Operability ($Sec(10\%), Ops(-x + y\%)$)	91
3.18	Interaction of <i>Pro or Student</i> and H_{16} with <i>number of family dependents</i> as moderator	94
4.1	Ranks for L_1A, L_1B, L_1C_half	108
4.2	Ranks for L_2A, L_2B, L_2C_half	108
4.3	Ranks for L_3A, L_3B, L_3C_half	108
4.4	Ranks for SL_1A, SL_1B, SL_1C_half	109
4.5	Ranks for SL_2A, SL_2B, SL_2C_half	109
4.6	Ranks for SL_3A, SL_3B, SL_3C_half	109
4.7	Wilcoxon Signed Rank Test pairwise risk aversion comparisons for L_1C (risk elimination) across the three groups.	114
4.8	Wilcoxon Signed Rank Test pairwise risk aversion comparisons for L_2C (risk elimination) across the three groups.	114
4.9	Wilcoxon Signed Rank Test pairwise risk aversion comparisons for L_3C (risk elimination) across the three groups.	114
4.10	Risk Aversion Boxplots for Lottery <i>Groups</i> $_{L_1C}$ across the three independent groups. Wilcoxon Signed-Rank Test significant values for comparisons of pairs: Groups A-C ($Z = -2.53$, $p = 0.034$), Groups A-B ($Z = -4.797$, $p < 0.01$).	114
4.11	Risk Aversion Boxplots for Lottery <i>Groups</i> $_{L_2C}$ across the three independent groups. Wilcoxon Signed-Rank Test significant values for comparisons of pairs: Groups A-C ($Z = -2.706$, $p = 0.02$), Groups A-B ($Z = -5.158$, $p < 0.01$).	115
4.12	Risk Aversion Boxplots for Lottery <i>Groups</i> $_{L_3C}$ across the three independent groups. Wilcoxon Signed-Rank Test significant values for comparisons of pairs: Groups A-C ($Z = -2.665$, $p = 0.08$), Groups A-B ($Z = -5.061$, $p < 0.01$).	115
4.13	Kruskal-Wallis Test for Risk Aversion between the three Groups.	116
4.14	Mann-Whitney Test for Risk Aversion between Groups.	117
4.15	Mann-Whitney Test for Risk Aversion between Groups.	117

LIST OF FIGURES

4.16	Mann-Whitney Test for Risk Aversion between Groups.	118
4.17	Mann-Whitney Test for Risk Aversion between Groups.	118
4.18	Mann-Whitney Test for Risk Aversion between Groups.	119
4.19	Mann-Whitney Test for Risk Aversion between Groups.	119
4.20	Mann-Whitney Test for Risk Aversion between Groups.	120
4.21	Mann-Whitney Test for Risk Aversion between Groups.	120
4.22	Mann-Whitney Test for Risk Aversion between Groups.	121
4.23	Mean risk-averse (positive) and risk-taking (negative) WTP of Professionals per Abstract Lottery. Bars represent participants' mean WTP minus the Δ (Expected Value) between initial and modified lotteries. . .	122
4.24	Mean risk-averse (positive) and risk-taking (negative) WTP of Professionals per Scenario Lottery. Bars represent participants' mean WTP minus the Δ (Expected Value) between initial and modified lotteries. . .	122
5.1	“Your current or last job role most closely resembles:”	131
5.2	“Which one of the following gambles do you instinctively prefer, at first glance?”	131
5.3	“In your opinion, how willing are Information Security Professionals to take risks in general?”	132
5.4	“How willing are you to take risks in general?”	132
5.5	“How willing are you to take risks in your [] role?”	133
5.6	“Are you less or more willing to take risks compared to your colleagues in your [] role?”	133
5.7	“Are you less or more willing to take risks in your [] role than in your personal life?”	134
5.8	“Do you think that your mathematical abilities are worse or better than the average person's in the general population? (E.g. with respect to probabilities and expected values)”	134
5.9	“In your opinion, which of the two attributes: Security or Operational Time, is perceived as more important by the following professional roles? (Participants that chose “Security”)	135
5.10	“In your opinion, which of the two attributes: Security or Operational Time, is perceived as more important by the following professional roles? (Participants that chose “Operational Time”)	135
5.11	“Imagine you are responsible for the Information Security budget; you have to consider potential information security threats and take an approach for protecting assets to an optimal level. Evaluate and rank the following decision criteria in two groups: the most important decision criteria and the criteria of secondary importance:”	137

LIST OF FIGURES

5.12	“Which of the following decision criteria, for protecting assets to an optimal level, do you think that you are mostly focused on or worried about as a result of your [] role?”	137
A.1	The “other-evaluation and behaviour” hypothesis statement is randomly presented to half of the participants.	169
A.2	The first task that is presented to participants involves five comparisons between lotteries. The first comparison is presented below.	169
A.3	In the next task, participants are asked to state their willingness to pay in order to avoid three lotteries of the following form.	170
A.4	Relative importance between security and operations is tested by a series of questions with the following design.	170
A.5	Subsequent questions are dynamically formed by the choices of participants.	171
A.6	Similarly to a previous section, the following questions elicit willingness to pay in order to avoid lotteries.	171
A.7	This screenshot shows an example of willingness to pay stated by a participant (presentation of this part is randomised between: risky lotteries being presented first and being followed by ambiguous lotteries, or vice versa).	172
A.8	The next section contains the mechanism for measuring relative loss aversion in either security or operations, based on previous choices of the participant.	172
A.9	The final section comprises the survey and demographic questions. . . .	173
A.10	Each participant is informed about the payment procedure.	173
A.11	The final payment is presented to the participant.	174
A.12	In the beginning of the experiment participants are randomly placed into one of the three treatment groups (here we have the “Losses frame group”).	242
A.13	Indicative lotteries that participants have to make risk decisions on. . .	243
A.14	Participants are presented with the lottery that will produce their payment, without knowing it.	243
A.15	Instructions given for the second part of the experiment.	244
A.16	WTP for probability reduction.	244
A.17	WTP for loss reduction.	245
A.18	WTP for avoiding the lottery completely.	245
A.19	Instructions for the final part of the experiment.	246
A.20	WTP for probability reduction in a scenario.	246
A.21	WTP for loss reduction in a scenario.	247
A.22	WTP for avoiding the lottery completely in a scenario.	247

A.23 Information given regarding the payment method.	248
A.24 An indicative payment message.	248
A.25 Demographics and survey.	249
A.26 End message.	249
A.27 Experiment Flow (Qualtrics Software [3]).	250

List of Tables

2.1 Properties of the Expected Utility Hypothesis	41
2.2 The Four-fold Pattern of Risk Attitude	48
3.1 Initial question of Scenario 1: “Which one of the following measures do you prefer?”	70
3.2 Scenario 2 template question	71
3.3 One-Sample t-test for between-subjects risk aversion	78
3.4 Lottery comparisons and accordance with heuristics	82
3.5 Lottery comparisons and willingness to pay inconsistencies.	84
3.6 Security VS Operability preference across Security Job Titles	89
3.7 Spearman’s correlation coefficients for General Risk	94
3.8 Kruskal-Wallis Test with dependent variable WTP and 4 Educational levels	95
4.1 Initial and adjusted lotteries with probability p and loss x . ΔEV is the expected value difference between initial and adjusted lottery.	108
4.2 WTP mean values for all lotteries and Wilcoxon Signed Ranks Test for pairwise comparisons between the following within-subjects conditions: Probability Reduction (lotteries L_iA , SL_iA), Outcome Reduction (lotteries L_iB , SL_iB) and Risk Elimination by WTP (lotteries L_iC_half , SL_iC_half).	110
4.3 Wilcoxon Signed-Rank Test for pairwise comparisons of abstract lotteries between the within-subjects conditions of probability reduction (L_iA) and outcome reduction (L_iB).	111
4.4 Wilcoxon Signed-Rank Test for pairwise comparisons of scenario lotteries between the within-subjects conditions of probability reduction (SL_iA) and outcome reduction (SL_iB).	112

LIST OF TABLES

4.5	Kruskal-Wallis Test for comparing WTP mean differences across the three independent framing groups (see also Section 4.3.3.1).	113
4.6	Mean differences of risk aversion values $RA_{Groups_L_i}$ from test value zero with the one-sample t-test ($TestValue = 0, N = 78$).	123
4.7	Mean differences of risk aversion values RA_{L_i} and RA_{SL_i} from test value zero with the one-sample t-test ($TestValue = 0, N = 78$).	123
5.1	Wilcoxon Signed Ranks Test for pairwise comparisons of decision criteria between hypothetical scenarios and professional-role questions.	138
A.1	H1 Instrument	164
A.2	Potential Outliers ($ z > 1.96$) for the z-scores of all outcome variables	187
A.3	Mann-Whitney U Test for Order Effects	188

Publications

This thesis is partly based on the following publications:

1. K. Mersinas, B. Hartig, K. M. Martin and A. Seltzer. Experimental Elicitation of Risk Behaviour amongst Information Security Professionals. *Workshop on the Economics of Information Security (WEIS)*, TU Delft, Netherlands, 2015.
2. K. Mersinas, B. Hartig, K. M. Martin and A. Seltzer. Measuring Attitude towards Risk Treatment Actions amongst Information Security Professionals: an Experimental Approach. *Workshop on the Economics of Information Security (WEIS)*, UC Berkeley, California, 2016.
3. K. Mersinas, B. Hartig, K. M. Martin and A. Seltzer. Are Information Security Professionals Expected Value Maximisers?: An Experimental and Survey-based Test. *Journal of Cybersecurity*, 2016; doi: 10.1093/cybsec/tyw009.

List of Abbreviations

CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Conjoint Measurement
CPT	Cumulative Prospect Theory
CSO	Chief Security Officer
EUT	Expected Utility Theory
EV	Expected Value
FFP	Four-fold Pattern
IRR	Internal Rate of Return
IT	Information Technology
NPV	Net Present Value
PT	Prospect Theory
ROI	Return of Investment
ROSI	Return of Security Investment
WTP	Willingness To Pay

Introduction

Contents

1.1	Motivation	18
1.2	Overview of Methodology	22
1.3	Organisation of the Thesis	23

1.1 Motivation

The topic of this thesis is the examination of behavioural traits that individual professionals and practitioners exhibit when they make decisions in the inherently risky and uncertain field of information security. The issues of particular interest are how information security professionals perceive risk, how they act in order to minimise or avoid risk, and whether behavioural biases adversely affect professionals' decisions.

Decision- and policy-makers are engaged in a constant effort to limit losses due to information security breaches. New regulations, policies, technical and operational measures are implemented in an attempt to minimise the exposure of organisations and governments to cyber threats. Spending on protective measures and mechanisms for information security is a big issue for most organisations. Specifying the optimal level of information security investment is not an easy task for security professionals. Reports show that defensive information security measures are increasingly adopted by businesses; nevertheless, the cost of security breaches either remains at high levels [110] or has been growing [4, 100]. However, insufficient expenditure on information security is considered as one of the main obstacles that security professionals face [4]. Optimising security investment level is crucial, but hard to achieve, and requires a balance between overspending and insecurity.¹

It might be expected that the existing plethora of best practices and standards for

¹When it comes to cybersecurity survey data interpretation should be careful, as contacted and responding populations can lead to unrepresentative samples [61]. Also, surveying rare events is by default problematic.

1.1 Motivation

managing information security systems would allow for investment decisions to be objectively evaluated and justified. However, there is a lot of space for subjectivity and judgement in today's information security environment. A generalised example that sketches the decisions an information security professional faces is the following. An information security professional needs to protect national or organisational assets of specific value against various threats. Therefore, she has to decide the amount of protective investment that is required to be spent in order to avoid unwanted losses caused by security breaches or failures. The professional possesses historical data on the frequency of various threats materialising, but data provides only an estimation of threat probabilities. So, it is up to her to decide and propose the exact investment level for minimising expected losses. In order to make an informed decision, she conducts an assessment on the vulnerability of the assets under protection. She needs to decide whether additional security controls are needed based on the expected value of loss. She might consider accepting the risk and not invest or she might propose investing in security measures for reducing the identified vulnerability. Alternatively, she can choose to implement measures for containing the potential damage in case it occurs, instead of making the asset less vulnerable. Finally, she can buy insurance in order to transfer part of the identified risk.

Using historical data as predictors on security events can be considered as the most objective and reliable approach for making informed decisions on the level of investment in information security. Such an approach allows for estimating the probability of threats and their potential impacts. The probabilities of specific events, along with the loss that an organisation might suffer, determine the expected losses associated with various threats. For the purpose of providing evidence that can fortify organisations more effectively, notification of cyber breaches is enforced by laws and regulations, such as the California Security Breach Information Act [38] or the EU General Data Protection Regulation [49]. However, such historical data is usually incomplete and decisions have to be made in fundamentally different contexts with dissimilar requirements. So, relying only on existing data for educated investment decisions is likely to produce sub-optimal decisions. Information security professionals have to face the ambiguity and uncertainty that missing or incomplete information bears and make decisions on security investment by using their preferred methodologies.

There is a number of approaches followed by professionals. For example, cost-benefit analysis [72] as well as risk-management resource-allocation techniques [79] constitute widely accepted approaches to the problem of investment levels. There are variety of models used by professionals including: Net Present Value (NPV), Internal Rate of Return (IRR), Return on Investment (ROI) and Return on Security Investment (ROSI) [19, 57, 73, 101, 124]. NPV is a metric which sums up investment gains per time period and subtracts the cost of investment from these gains. The metric includes a discount

1.1 Motivation

rate factor per time period, which describes the decreasing trend of investment gains per time period. IRR is the specific discount rate which makes NPV equal to zero. ROI is another measure which evaluates the efficiency of an investment; basically it is the difference between the gains from an investment minus the investment cost, divided by this investment cost. ROSI is essentially the application of ROI in the domain of security; namely, instead of gains it uses monetary loss reduction which is estimated by the reduction in the annual loss expectancy by a threat achieved by investing in a security measure. Importantly, all these metrics use expected gains or expected reduction of losses.

But, since there is no dominant model for decision-making in security [123], professionals are encouraged to choose their own appropriate risk analysis and assessment methods [34, 81] to match the needs of their organisations.

However, all methodologies which try to assess risk in a quantitative fashion are subject to three significant limitations [57]:

1. Many approximations are involved in the process, e.g. due to ambiguity and unknown risks;
2. As a consequence, these approximations can be biased by the decision-maker's perception of risk, and;
3. Involved calculations conducted by the decision-maker can be easily manipulated.

2

Subjectivity of risk perception and the lack of a predominant bounding economic model for *deciding* and *justifying* security investment, imply that the decision-maker's preferences and risk attitude, may have important effects on decisions.

Individual *risk perception* refers to people's judgement and evaluation of a hazard. *Risk attitude* is the individual's intention to evaluate and act on a risky situation [127] and can be defined as "a chosen response to uncertainty that matters, driven by perception" [77]. Perception of risk and attitude towards risk are concepts that have been extensively studied in the field of behavioural economics [40, 91, 105] revealing various biases and heuristics, i.e. simple rules, that individuals use when making decisions.

Coming back to the aforementioned example, we can highlight various points that allow for subjective approaches. For example, the professional's attitude towards risk can be differentiated depending on the probability of a threat materialising, and also on the

²For example if the expected annual frequency of occurrence of a threat is estimated to be, say, ten, it can be easily deflated to eight or exaggerated to twelve, for serving the decision-maker's personal agenda. Such a manipulation would also bear changes in costs.

1.1 Motivation

expected damage to be incurred. When a threat bears potential catastrophic outcomes, the attention of the professional might be disproportionately focused on the worst-case outcome, and hence she might be willing to spend more in order to be on the safe side, even if the probability of such an event is negligible. In other cases, she might diminish the urgency of quite probable threats or consider small losses inevitable. The professional might have preferences over the available actions, even if the expected value of the alternative choices is the same, a fact that would imply the existence of different preference criteria. Another factor the professional has to take into consideration and which can potentially affect her decision is the balance between the level of protection and operational efficiency. The professional can view protection of the assets as a necessary cost subtracted from the budget, or she can view it as an investment with business return or other benefits. The classification of protection as either gains or losses may affect her willingness to invest.

The final investment decision that the professional makes is potentially influenced by these factors, including her individual attitude to risk. Importantly, the decided level of investment has to be communicated and justified to other parties in the governmental or organisational structure; these parties may lack the expertise necessary to understand her suggestions. Such a possibility might cause the security professional to either exaggerate or deflate her initial proposals in order to make them seem justifiable. Thus, a variety of potentially influential factors, the amount and quality of available information and individual perception, all potentially affect decisions. Consequently, information security professionals have to rely on their judgement and thus, their preferences and biases are ultimately inserted in the decision-making process.

Expected utility theory is the standard normative approach to decision making which states that for decisions which are made frequently, a rational decision maker should maximise expected gains. We use this approach, as it is aligned with the widespread industry practice [57]. Maximisation of expected profits, or, quite often in the context of information security, minimisation of expected losses constitute strategic goals for organisations. These goals can be achieved, amongst other actions, by objectifying security investment decisions. In this research we take an experimental approach in order to examine risk perception, risk attitude and security-related preferences of active information security professionals. In particular, we investigate whether the inherent subjectivity in information security decision-making causes systematic violations of expected value maximisation and produces behavioural biases which make professionals' decisions suboptimal. We also examine whether risk behaviour of professionals differs from the behaviour of a student sample, due to context parameters or professionals' exposure to risk. We present related literature in Section 2.1.4, however, to the best of our knowledge, this kind of research has not been studied to an adequate extent. The strengths and limitations of the research approach are discussed in Section 2.2.

1.2 Overview of Methodology

For the purposes of this study we conduct a series of experiments and surveys. A sample of active real-life information security practitioners and professionals is drawn from current and former students of the master's degree in Information Security from Royal Holloway, University of London (RHUL). These professionals have significant experience across a variety of roles in the industry, as described in detail in the experiments of Chapters 3 and 4 (see Sections 3.2.2 and 4.2.2). Another sample of volunteer students is drawn from individuals registered in the database of the Laboratory for Decision Making and Economic Research at RHUL.

We ask participants to state their willingness to pay in order to avoid lotteries which have negative-only outcomes. Except for abstract lotteries, we use security-scenario lotteries in order to simulate the context of information security. This way, we measure the attitude of subjects towards risk. A variety of lotteries with different levels of probabilities and outcomes is used. Some lotteries have fixed probabilities and outcomes and others involve ranges of probabilities or ranges of outcomes or both. This allows us to examine behaviour towards ambiguity. We devise lottery-comparison tasks in order to elicit risk preferences of participants. We present the same problems in a variety of ways and we separate subjects into differently-framed condition groups for exploring potential framing effects. It should be mentioned that in this research, the approach followed is the traditional assumption that the preferences of decision-makers are revealed through their choices.

Survey results are used in combination with experiment findings. Except for demographic information, the surveys involve problems presented as information security scenarios, in order to examine decisions in context. Participants also reply to questions regarding risk perception in general and in relation to their professional roles. Priorities, decision criteria and role-dependent risk preferences are also reported by the sample of professionals.

Subjects are informed about the anonymised processing of data, which is used only for the purposes of the study, before they consent in taking part in the experiments. They are also informed about the maximum amount of payment that they might receive³. It is explained to participants that they will be paid based on their performance. The amount of payment is randomly generated by a computer function which simulates one of the lotteries that participants choose during the experiments. Payment is sent to participants in the form of an Amazon gift certificate, via the Amazon website of their preference.

³For example, participants are informed that they can earn up to 13 and 10 USD in the experiments of Chapters 3 and 4, respectively.

1.3 Organisation of the Thesis

Whenever possible, we use non-parametric statistical tests, because they involve fewer assumptions than parametric tests. All experiment tasks are designed and tested against order effects. In order to exclude order effects from the experiments we conduct the following steps. First, we randomise the order of questions so that participants, for example, are not presented with the same types of lotteries in the same sequence. We also randomise all treatment groups in which participants are assigned to. Secondly, we examine whether there are significant differences in risk behaviour amongst the random groups. No order effects are detected in the research.

1.3 Organisation of the Thesis

The rest of the thesis is organised as follows.

Chapter 2. In this chapter we describe the increasing importance of decision-making in information security. Fundamental notions of information security risk management are presented, along with potential biases related to the security environment. We also provide the theory and the models used in experimental and behavioural economics for the elicitation of systematic patterns in individual risk behaviour.

Chapter 3. This chapter explores risk attitude of information security professionals under risk and ambiguity by the use of an experiment and a survey. We also test other hypotheses in this experiment, namely worst-case aversion and other evaluation ambiguity aversion. A sample of students is additionally used in the experiment in order to contrast behaviour of professionals.

We ask participants about the amount of money they are willing to pay in order to avoid unfavourable lotteries. This way we elicit their attitude towards risk across various levels of probabilities and negative outcomes. Other tasks require that participants choose between two lotteries. We do not trace enough evidence to support other-evaluation ambiguity aversion or worst-case aversion. However, we detect systematic violations of expected utility theory. Risk behaviour of professionals is found significantly different from that of students in various ways. Professionals are better than students at minimising expected losses, but they are equally, and occasionally worse, than students in being susceptible to preference reversals when presented with the same problems framed in different ways. These findings imply that professionals' involvement with risk might objectify their decisions to a certain extent, however some biases are manifested equally amongst professionals and students. Perception of probabilities is also estimated as being more distorted by professionals than by the student sample. Professionals are also found significantly averse towards ambiguity. The former finding might indicate professionals' limitations in making objective decisions and the latter their inclination to

1.3 Organisation of the Thesis

accurately specify risks. Lastly, we devise a mechanism in order to measure prioritisation of professionals over the system attributes of security and operability. The elicited preferences are shown to depend on professionals' job positions. Both professionals and students are found to systematically deviate from expected value maximisation.

Chapter 4. In this chapter we describe an experiment that investigates preferences of information security professionals related to the risk management process. In particular, we examine preferences of professionals over risk treatment actions and their behaviour under different framing conditions.

Professionals are again asked about their willingness to pay (WTP) in order to avoid a series of negative-outcome lotteries or modify the stakes of lotteries into being more favourable. We elicit characteristic preferences for specific types of lottery modifications. Additionally, professionals are asked to make investment decisions in hypothetical information security scenarios. Professionals systematically prefer to reduce losses rather than the probabilities associated with these losses in these scenario-lotteries. Three treatment groups are created randomly, presenting participants with risky choices framed as gains, losses or individually separated losses. Professionals reveal a distinct behaviour for eliminating losses: they are more risk-averse in the gains-group than in the losses-group and more risk-averse when losses are reduced from individual budgets than when they are subtracted from a single budget. However, the possibility of eliminating risk completely does not change professionals' risk behaviour relatively to modifying risk.

Chapter 5. This chapter presents the potential implications of research findings, along with a survey regarding professionals' risk-related perceptions. We interview three renowned information security experts and evaluate the potential impact of the research findings in real-world security environments. We discuss recommendations for de-biasing suboptimal security investment decisions.

Chapter 6. Finally, we present the conclusion of the thesis.

Background

Contents

2.1	Information Security	25
2.1.1	The Importance of Information Security	25
2.1.2	The Information Security Profession	26
2.1.2.1	The Risk Management Process	28
2.1.2.2	Threats, vulnerabilities and losses	30
2.1.3	Behaviour and Decisions in Information Security	31
2.1.4	Behavioural and Economic Approaches to Information Security	37
2.2	Economics and Behaviour	38
2.2.0.1	Experimental Elicitation of Risk Attitude	39
2.2.0.2	Surveys	39
2.2.1	Decision-making Models of Risk Behaviour	40
2.2.1.1	Prospect Theory	46
2.2.1.2	The Machina Triangle	49
2.2.1.3	Saliency Theory	52
2.2.1.4	Uncertainty and Ambiguity	55
2.2.2	Modelling Investment Decisions	56
2.3	Summary	60

2.1 Information Security

2.1.1 The Importance of Information Security

Our age has been characterised as the “Information Age”. The products and by-products of our daily activities produce a vast amount of digital data. All this data can be viewed from the perspective of an individual’s daily activities. We connect to the Internet, exchange messages, upload photos and videos, use GPS devices, are captured by cameras, record our daily jogging exercise and our phones, watches, televisions and

2.1 Information Security

even our cars are connected to networks. It has been estimated that since 2010, humanity has been producing more data per day than from the beginning of time until the year 2003 [136]. At the same time, we want our communications to remain private, our personal data stored on our computers, tablets and mobile phones to be unreachable by strangers, and our blood test results to be shared only with medical personnel. We also expect that traffic lights operate reliably, electricity and water supplies are available at all times, and that we are able to use our technology and devices whenever we find it convenient. We do not want someone posting messages on social media using our name, nor have our credit card details stolen while we shop online.

On the other hand, there is a corporate perspective of information security, which is under examination in this research. Organisations in every business sector have a goal to meet their business objectives. The opportunities that businesses have to take or create, inherently include information security (or cybersecurity) risks. In this sense, information security risk management plays a crucial role for organisations, because it protects valuable assets, it secures communications, it maintains information trustworthy, it keeps services available to clients and provides a variety of security services. Thus, the well-being and progress of all kinds of organisations relies, to some extent, on managing information security risks. But, the primary goal of businesses is to maximise their expected profits and, at the same time, minimise their expected losses. An organisation's investment in information security measures ultimately needs to serve this purpose.

2.1.2 The Information Security Profession

Professionals involved in information security face difficult decisions. They have to select appropriate measures relating to security technology, security services, awareness training programs, forensic services and regulatory compliance amongst other issues. Allocating and justifying the optimal amount of investment for each measure is not an easy task. The reasons are mainly the uncertainty that pertains potential losses associated with security breaches and the ambiguous nature of the associated threats and vulnerabilities. Decisions made by security professionals are crucial; monetary losses caused by security breaches can have a devastating impact on the continuity, recovery, the brand value and reputation of the business, and ultimately, on the very existence of an organisation [123, 124]. On the other hand, demonstrating a low number of security breaches can provide the organisation with a commercial advantage over its competitors [8].

Excluding reputation which can, for example, reveal the security posture of an organisation, security can be often viewed as a gamble that professionals have to take. In

2.1 Information Security

this gamble, the organisation either suffers a loss or, in the best-case scenario, loses nothing. In this sense, security controls are tools for loss minimisation, and a “security gamble” yields only non-positive outcomes. This fact diversifies the information security investment context from the usual economic framing of choice outcomes as gains or losses.

The term “investment” in information security was introduced in previous sections but, it is important to note, that organisational culture still largely treats security as an overhead and not as an investment [120]. This view constitutes an obstacle in professionals’ attempts to justify investment in security measures.

For the purpose of this research we categorise information security professionals into four main roles:

- Senior executives, e.g., Chief Executive Officers (CEOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Security Officers (CSOs), etc.
- Managers, e.g., Project Managers, IT Directors, Security Managers, etc.
- IT & Security professionals, e.g., Security Officers, System Administrators, Information Analysts, etc.
- Compliance, Risk and Privacy professionals, e.g., Consultants, Auditors, etc.

The role of security professionals, except for choosing appropriate protective mechanisms, involves prioritising and balancing attributes of the system under protection. For example, one of these characteristics is the notion of trade-off between security and operability (e.g. operational time) in a security environment. Considered through this prism, the decision-maker has yet another dimension to the problem to consider before investing.

Another factor which might influence the decision process is the position of the decision-maker in an organisation. For example, top-down approaches to risk management initiated from higher management and shareholders have entirely different results to bottom-up approaches, which are pushed “upwards” from information security personnel to management. There are some interesting findings regarding the correlation of professional roles with preferences of professionals, as will be presented in the following chapters (see Chapter 3). These issues are dynamic and constantly evolving. Reports show a shift from traditional decision-making conducted by security and IT managers towards a framework that involves senior management as well as financial and operational managers in the decision process [76]. Thus, information security professionals are not necessarily the only contributors to the information security risk management

2.1 Information Security

process of an organisation, nor have they the final word on investment decisions. However, their opinion is highly influential.

Investment in security mechanisms is decided through the risk management process, as is explained in more detail in Section 2.1.2.1. At the heart of risk management lies risk assessment and its countless approaches. In order for a quantitative assessment of risk to be conducted, threats have to be identified, existing vulnerabilities need to be evaluated, probabilities have to be assigned to each potential threat manifestation, and corresponding losses need to be estimated. A more detailed description of threats, vulnerabilities and risk is presented in Section 2.1.2.2. In Section 2.1.3 we describe a number of information-security-related economic and behavioural hypotheses which are examined in this study.

2.1.2.1 The Risk Management Process

We provide the definitions and approach of the International Organization for Standardization (ISO) regarding the risk management process in information security. ISO is probably the most widely accepted, independent, non-governmental membership organisation and largest developer of international standards. The ISO/IEC 27000 series of standards is dedicated to information security and is published collaboratively by ISO and the International Electrotechnical Commission (IEC). These standards have been embraced by the information security industry [83], and certification against certain standards in the series has been made mandatory by a number of governments worldwide.

Risk management is defined in ISO Guide 73 [80] as the “coordinated activities to direct and control an organization with regard to risk”. The overall process of risk management is defined as “a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk”. The set of activities that comprise the risk management process can be broadly categorised as either risk assessment or risk treatment. Risk assessment, consists of:

1. Risk identification: where threats and vulnerabilities are found, identified, and described.
2. Risk analysis: where the nature and level of risk is estimated.
3. Risk evaluation: where the risks are evaluated against the organisation’s risk criteria.

2.1 Information Security

All three phases of risk assessment require information security professionals' judgement.

Risk treatment follows risk assessment and consists of “what to do with the risks at hand”, e.g. implementing controls in order to reduce, retain, avoid, or share risks depending on expected costs and benefits [81]. Risk treatment is the final risk decision that needs to be taken or proposed by security professionals.

The four risk treatment actions are defined in the following way. Risk *reduction* or *modification* refers to the action of reducing the probability of loss, or the loss itself. The action of *retaining* risk, is the choice by which the decision-maker *accepts* the identified risk as it is. Risk *avoidance* is usually the business decision by which the scope of the organisation changes, and therefore there is no exposure to certain threats. Finally, risk *transfer* refers to the action in which risk is *shared* with some other party, usually by purchasing insurance.

It is widely accepted that “judgement” is not only unavoidable, but also necessary for managing risk successfully. There are two clear, albeit very general, suggestions in ISO 27005 [81] for efficient risk treatment:

- Judgement should be exercised in certain cases for the justification of decisions, and;
- Perception of risk by affected parties should be taken into account.

However, individual expert judgement cannot be easily “put into moulds” and worryingly has been shown to be far from optimal in many areas of expertise [60, 68], mostly because experts reveal subjective preferences, choice inconsistencies and cognitive limitations [141].

One further factor that needs careful consideration is how to find the “most appropriate ways to communicate risk” to involved parties [81]. However, just as there is no unified approach to measuring perceived risk, neither is there a well-defined methodology for risk communication. Importantly, the risk management approach and the individual behavioural traits might shape the preferences of professionals, making their choices sub-optimal. To our knowledge, behavioural issues associated with the decision points of the risk management process have not been extensively studied, especially, from the perspective of individual choices of information security professionals.

2.1 Information Security

2.1.2.2 Threats, vulnerabilities and losses

In order to perform quantitative risk assessment, information security professionals have to estimate the following variables, which depend on the given system under protection and the needs of the organisation. The following definitions are taken from ISO 27002 [82]:

- *Threat* is a potential cause of an incident that may result in harm to a system or organisation.
- Security *vulnerability* is a weakness of an asset or group of assets that can be exploited by one or more threats.
- *Risk* is the potential that a given threat will exploit vulnerabilities of an asset or groups of assets and thereby cause harm to the organisation.
- *Impact* is the result of an information security incident, caused by a threat, which affects assets.

Each potential information security threat i is assumed to have a corresponding probability of occurrence, i.e. a probability of manifestation, t_i . For each threat, the information system or organisation under protection has an associated probability of breach (vulnerability), v_i . The estimated impact (i.e. the outcome or loss) that the organisation suffers when a breach is materialised, is symbolised with x_i , for various outcomes; this is related to the value of the asset under protection. One approach is to assume that the total value of the asset will be lost in the event that a threat materialises [8].

- *Asset* is anything that has value to an organisation, its business operations and its continuity [82].¹

Threats are external, meaning they exist independently of any actions of the decision-maker, thus, their probabilities cannot be altered. By contrast, vulnerabilities are internal, meaning that their associated probabilities can be reduced by security investment decisions. In some cases, information security professionals do not target vulnerability probabilities v_i with their investment decisions, but instead aim to contain the potential impacts x_i .

The probability that a vulnerability is exploited allowing a threat to be realised, i.e. the risk, is $p_i = t_i \times v_i$. The various probabilities of risk p_i correspond to outcomes x_i . The expected value of the impact of an information security incident then is:

¹This definition is deliberately vague. Notably, an asset can be information, a physical item or software.

2.1 Information Security

Expected Outcome = $t_i \times v_i \times x_i$. In some cases, for the purposes of simplicity or abstraction, risk probabilities p_i can be used directly, allowing for the omission of t_i and v_i .

2.1.3 Behaviour and Decisions in Information Security

In this section we present a number of decisions that information security professionals have to make and the associated behavioural traits that they might exhibit.

Risk Aversion

The first trait that can be examined in the behaviour of information security professionals is attitude towards risk. That is, whether professionals are risk-averse, risk-neutral or risk-seeking when they face threats and potential losses. In this research we examine risk attitude by comparing professionals' willingness to pay in order to avoid unfavourable lotteries with the expected value of these lotteries. There might exist a number of factors that could cause decision-makers to deviate from expected value maximisation. For example, their risk behaviour might depend on the level of the threat probability and / or the magnitude of losses. Professionals might have a certain risk behaviour which is shaped by their involvement with information security. Such a behaviour might be different from the behaviour of the general population, due to the frequent exposure of professionals to risk.

Findings related to professionals' risk attitude are presented in Section 4.3.4; a comparison with the behaviour of a student sample is described in Section 3.3.1.

Ambiguity Aversion

Given that real-world decisions are ultimately at least ambiguous, a substantial amount of theoretical and empirical work has been focused on the observed phenomenon of the so-called ambiguity avoidance or ambiguity aversion. Very loosely, *ambiguity aversion* can be defined as the attitude of preferring specific probabilities over ranges of probabilities, i.e. preferring risky lotteries over ambiguous lotteries. Another definition for ambiguity is the lack of knowledge regarding various scenarios [48]. This is the most common situation in information security, where it is almost impossible to estimate the exact probabilities of threats and vulnerabilities.

There are a variety of psychological sources of ambiguity aversion which have been studied in the quest of explaining observed avoidance in decisions [50]. For example, self-evaluation and other-evaluation is a pair of hypotheses in which decision-makers anticipate future evaluations. Such an anticipation can either refer to decision-makers' own future evaluation about past choices, in a similar way to regret-aversion [102]. Or,

2.1 Information Security

alternatively, decision-makers might weight their choices by anticipating the evaluation of others, e.g. of peers and colleagues. Such a setting is common in organisations and information security environments.

Other-evaluation Ambiguity Aversion

The information security setting of the other-evaluation ambiguity aversion hypothesis can be a cooperation between a security professional and a senior manager. In an oversimplified version of the setting, the security professional proposes a security investment and the senior manager accepts or declines the proposal.

This setting places security professionals in a defensive position where they need to prove their competence by the soundness of their choices, as it is expected from them to make sound decisions for protecting the organisation's assets. This is a distinct characteristic of the security professional role. So, according to the other-evaluation hypothesis, decision-makers are ambiguity averse because they choose the most, a posteriori, justifiable option. For example, if a choice were between two risky lotteries it would be justified to choose the less risky lottery, in which case increased "riskiness" can be expressed by the mean preserving spread of a lottery [130]. In particular, if decision-makers prefer a lottery over its mean preserving spreads, then they are ambiguity-averse. Moreover, the measure for such aversive behaviour can be explicitly specified by the risk premium that the decision-makers are willing to pay, for not taking the gamble. If the dilemma were between a risky and an ambiguous lottery, then the most justifiable choice would be to choose the risky lottery. Accordingly, if the decision-maker were to decide between two ambiguous lotteries, then the less ambiguous one could be more easily justified to other parties. In this sense, other-evaluation leads to ambiguity aversion. It is reasonable to assume that this attitude should be manifested in information-security decision-making environments, although, as far as we are concerned, this aspect has not been studied. The other-evaluation ambiguity aversion hypothesis has been empirically reproduced and sustained as a purported psychological source of ambiguity [50].

Other approaches suggest that ambiguity is a second step in the decision process in which the less ambiguous option is chosen if all other alternatives are equally preferred (*forced choice*) [50, 126].

We present experimental findings that strongly support ambiguity aversion (see Section 3.3.1, but we find no evidence of other-evaluation ambiguity aversion (see Section 3.3.3). Possible implications of these results are discussed in Section 5.5.

Action and Inaction

Risk aversion and ambiguity aversion in other contexts have been shown to lead to

2.1 Information Security

the omission-bias [125], i.e. a reluctance of the decision-maker to act. Explanations of this bias include the perception that damaging omissions are preferred to damaging actions [142]. Another explanation is the belief that inaction does not cause outcomes. Security professionals have to justify their choices, but even before that they have to justify their position. It is doubtful that omission under risk and ambiguity could be justified as an information security strategy. This might well be the case even if inaction is the most beneficial option, because it is harder to justify. It is therefore expected that decision-makers behave in an “*anti-omission*” (commission) manner, in order to justify their role and position. At the end of the day, it is considered “better” to take measures for something that will never happen, than having omitted to take action for a security breach that did manifest. However, such a choice is not necessarily the one that minimises losses. For example, the option of buying insurance and thus transferring risk to another party, even if beneficial, could be less preferable as an option to professionals. Statistically significant findings of our second experiment may indicate the existence of such behaviour (see Section 4.3.1).

Gains and Losses

A common perception regarding the information security context is that outcomes belong in the *domain of losses*. That is, the best outcome is usually considered to be a zero loss and there can be no gain. This is a characteristic that differentiates decision-making in security from decision-making in other environments, e.g. a financial context, where losses are mirrored by gains. We test whether such a perception of security has an effect on professionals’ risk attitude by contrasting this view with an approach to information security as an activity with potential return on investment (see Section 4.3.3).

Focusing on outcomes

A bias towards the *outcome* of a decision, in which the decision-maker distinctively ignores the decision *process* has been reported. Subjects that manifest this bias, a posteriori overweight the quality of thinking and the competence of the decision-maker whenever the result-outcome of the decision turns out to be beneficial, or when the alternative that was not chosen would have been damaging. Such a bias is present even if experimental subjects believe that evaluation of choices should not only depend on the outcomes, but also on the process [22].

Another dimension on the focusing-on-outcomes phenomenon is the possibility that professionals overestimate the importance of impact and, at the same time, underweight the probabilities of threats and vulnerabilities which produce these outcomes. This behaviour might be related to the information security dilemma between proactive and reactive measures [144, 23]. That is, attention can be targeted towards reducing the

2.1 Information Security

vulnerabilities of the system under protection or, since it is impossible to eliminate risk completely, to minimising the extent of damage, in the event that a security breach occurs. The former case is the traditional approach to security and aims to reduce the probability of risk, whereas the latter is concerned with minimising the losses associated with risk. Although for real-world security implementations it is recommended that both these approaches are taken, it is possible that security professionals have their own subjective disposition. Slovic [140] proposes the existence of an experiential, as well as an analytical, form of thinking involved in decisions (proportion dominance) which causes a preference for reduction of probability of loss instead of loss itself. Our research findings relating to these questions are presented in Section 4.3.2 and are also discussed in interviews with security experts in Section 5.4.

Worst-case thinking

The *hostile nature* hypothesis refers to considering a non-random way by which uncertain events occur [158]. In this hypothesis, less favourable outcomes are perceived as more likely to happen than beneficial ones. Similarly to the hypothesis of hostile nature there is *worst-case thinking* as an aspect of information security decision-making. This type of thinking implies that decision-makers focus on the “worst possible outcome and then act as if it were a certainty” [135]. Decision-makers imagine more vividly the less probable events with potentially more catastrophic outcomes and magnify the probability of such low-expected occurrence events. This could be related to a number of decision-making heuristics such as *representativeness* and *availability*. Representativeness refers to “the degree to which an event (i) is similar in essential characteristics to its parent population, and (ii) reflects the salient features of the process by which it is generated” [89]. This heuristic might cause an event to be perceived as more likely by the decision-maker, because it is more representative. Availability is the heuristic by which we bring the “most available” comparable example in our minds in order to judge some information. The heuristic gives more weight to recent and vivid information, at the expense of older information which did not have the same impact on the decision-maker’s memory [69, 149]. For example, after a specific security breach is publicised, most security professionals overreact by overestimating the probability of this incident manifesting.

On the other hand, worst-case thinking is a sort of “validation of ignorance”, in the sense that individuals are reluctant to focus on what they know, but exaggerate the importance of speculation. This means that information that decision-makers have access to is not fully used or, even worse, is underestimated for the sake of missing information. In other words, there is a tendency to focus on uncertain events, with immeasurable, but in any case small, probability of occurrence. Therefore, this type of thinking implies an overweighting of low-probability events. There seems to be some

2.1 Information Security

psychological source (or sources) which enlarges the probabilities of seldom occurring events and attracts the attention and mental focus of security decision-makers. Focusing on such events, along with the underweighting of more common events, could be viewed as an attitude towards uncertainty, or an attitude generated by uncertainty, if disproportionately focused attention were to be positively correlated with the degree of uncertainty that the decision bears.

The approach that is chosen in this research in order to examine worst-case thinking is salience theory [32]. Salience theory states that it is outcomes which are sufficiently diversified from the rest that disproportionately draw the attention of the decision-maker. In a context that bears large losses, a catastrophic outcome can be perceived as “salient” by the decision-maker. High-impact publicised security breaches can be overweighted in professionals’ perception, leading to over-investment in particular measures and jeopardising optimality of security investment.

Salience theory is presented in detail in Section 2.2.1.3 and experiment findings relating to this type of bias are described in Section 3.3.2 .

Data on Past Security Events

In the information security environment, one could claim that there is always some sort of information available to aid the decision-maker. As has been already mentioned, information might be available from historical data, personal experience or information security surveys. Based on the reasoning of Florencio and Herley [61] surveys that report security breaches can be misleading and are not trustworthy. The main argument is that even if the contacted population were a representative sample of the whole population, the final respondents choose to participate in the surveys for their own specific reasons, which makes the sample biased and diminishes the reliability of results.

Reliability of such data is increased with disclosure laws which enforce breach notification, such as the California Security Breach Information Act [38] or the EU General Data Protection Regulation [49]. But, even if such data on past security events is reliable, information of this kind can act as an *anchor* for the decision-maker. That is, available information can become a potentially unjustified reference point (the “anchor”) for subsequent decisions. This reference point can be shaped by the aforementioned *availability* of information, meaning that security incidents which make headlines are more likely to make a strong impression on professionals’ minds.

Security VS Operability

As mentioned in the previous section, information security professionals need to decide on the prioritisation of system attributes, depending on the context of implementation.

2.1 Information Security

One of these decisions is the point of balance between security and operability. Placing more security controls might always be desirable from a security perspective, but such an action usually implies reduced operability. Speed of operations, operational costs and user convenience are factors which need to be evaluated by professionals against the security benefits of implementing specific security measures.

We devise a mechanism in order to examine professionals' preferences between security and operability (operational time). Findings are presented in Section 3.3.4.

Professional Role

Another factor which might influence risk-related decisions of professionals is their professional role. Risk can be perceived differently by senior executives of an organisation than is perceived by Information Technology (IT) personnel or consultants. Individuals who have the ultimate responsibility and make the final decisions for protecting an asset (risk owners) can react to potential threats in a manner systematically different from that of professionals who make suggestions for protecting this asset. Prioritisation of decision criteria in order to mitigate or avoid risk can also be perceived differently, depending on the professional position of the decision-maker. The level of influence of the various professionals involved, and the degree of consensus needed for deciding on security investment, differs between organisations. However, it is important to be able to distinguish potentially misaligned risk perceptions.

We report the influence of professional roles on preferences and risk perception in Sections 3.3.4 and 5.3.

Preferences over Risk Treatment Actions

Decision-makers in information security can also have preferences regarding how to treat risk. Risk treatment is the decision regarding "how to deal with the identified risk". Risk can be avoided, transferred, modified or accepted, as described in Section 2.1.2.1. It could be the case that decision-makers are biased towards some of these actions at the expense of others, even if the expected outcome of the alternatives is the same. We present evidence of such a bias in Section 4.3.1.

Framing

Framing is a phenomenon which transcends the majority of real-world decisions. Presentation, and most importantly, the context of a decision is known to influence individuals when they make choices [150]. An influential type of framing is the perception of risky or ambiguous decisions as either gains or losses, as already mentioned. In such situations decision-maker's risk attitude changes. The aforementioned view of information security investment as potential business gain instead of a necessary cost can shift

2.1 Information Security

risk attitude of decision-makers, as our experimental findings of Section 4.3.3 strongly suggest.

Framing effects related to the presentation of problems are also detected in the form of preference reversals between willingness to pay and choice tasks. This can be a very common issue in information security, although professionals would like to think the way a problem is presented does not affect their decisions. These findings are presented in Section 3.3.2.2.

The previous examples and characteristics of information security decision-making reveal a variety of factors and the complexity of the topic. Decision-makers in information security can become risk seeking, but they can also act in a risk-averse fashion, being repulsed by ambiguity. They might be eager to act and invest in security measures due to the nature of their role. They are prone to behavioural biases and subjective evaluations. An examination of certain behavioural patterns, attitudes towards risk and an analysis of opposing behavioural components is presented in the following chapters.

2.1.4 Behavioural and Economic Approaches to Information Security

The importance of the economics of information security with extensions to behavioural aspects has been highlighted in various papers of Anderson and Moore [11, 12, 14, 15, 16]. The main point of their approach is to highlight the inherent difficulties in information security caused by misaligned incentives of the involved parties. Subsequently, studies on specific behavioural aspects of information security, such as privacy [7], have become more frequent. A significant amount of research has been focused on the behaviour and incentives of users [53, 71].

Outside of the information security field, behavioural economics has revealed a number of “paradoxes” or systematic violations of expected utility theory [155], showing that the assumed rational-agent “homo economicus” is not observed empirically [40, 91, 105] in decisions that individuals make. An attempt to connect information security issues with potential heuristics and biases decision-makers exhibit is sketched by Schneier, in the “psychology of security”, in which issues related to the perception of risk and uncertainty are described [134].

There are studies that use an expected utility theory [51] as well as prospect theory approach to security [154]. Schroeder uses prospect theory and also explores the dichotomy between security and operations in military-context empirical research [137]. Insights from psychology and sociological factors, as well as biases in security, are presented by Baddeley [20]. There has been research focus on the decision-making process of security professionals from a decision support system point of view [30]. Shiu et al.

2.2 Economics and Behaviour

conduct an experiment on security professionals with economic framing controls, revealing the existence of the confirmation bias [21]. Other biases, like the status quo and present bias have been specifically targeted, albeit from a privacy perspective [5, 6, 7]. The effect of biases on security design has also been explored [65]. Timing preferences about security investment have been studied by Ioannidis et al. [84].

Researchers have focused on the decision-making process [6, 84] and proposed models for security investment [72, 41]. The majority of these studies propose formal models for optimising the level of security investment. However, real world investment can be environment-specific and might depend on the organisational structure [24], as well as on the roles of the involved risk owners and stakeholders [25]. This fact implies that formalising investment decisions might be of limited practical value. Risk management and policy [31, 73, 86] constitute the framework in which investment decisions are made, and thus can be considered as another important aspect of security investment.

Decisions are inherently related with perception of information security risk, and it has been pointed out by researchers that such a perception entails a variety of dimensions [85, 119]. However, the empirical examination of risk perception and risk attitude of active information security decision-makers can greatly contribute to de-biasing and optimising security investment. To the best of our knowledge, this aspect has been relatively less studied.

2.2 Economics and Behaviour

The approach of this research is interdisciplinary between Information Security and Economics. In particular, for the purpose of examining how information security professionals react to risk, and which biases potentially make their decisions suboptimal, we use methodologies from behavioural and experimental economics.

The scope of behavioural economics is to increase “the explanatory power of economics by providing it with more realistic psychological foundations” [47].

Perception of risk and attitude towards risk, as well as violations and limitations of “rational choices”, have been extensively studied in behavioural economics [91, 105, 138, 139]. Behavioural research has revealed systematic violations of expected utility theory [155] suggesting that decision-makers as rational agents are rarely observed in real-world decision-making scenarios. By contrasting individuals’ choices with predictions of expected utility theory, we discover a variety of biases and systematic errors in information security decision-making.

In this section, we describe how preferences of security professionals can be elicited

2.2 Economics and Behaviour

and we present the core theories on which we base our approach. We also propose an approach for modelling information security investment decisions.

2.2.0.1 Experimental Elicitation of Risk Attitude

In this research risk preferences of subjects are elicited by online experiments. Risk preferences of individuals are specified by the extent to which they are “willing to take on risk” [43], that is, they are expressed by their attitude towards risk. *Willingness-to-pay* (WTP) in this study is treated as the maximum amount that the individual is willing to sacrifice in order to avoid an undesirable event. We use WTP as a technique to model choices in the experiments. Subjects reveal their preferences by stating their WTP in order to avoid risky or ambiguous lotteries with negative outcomes across a variety of experiment designs and conditions. Such an approach also reveals the subjects’ *belief* about how plausible events are to occur ([33], Ch.15.2.2). It should be noted that all lotteries used in the experiments are decision-based, with no feedback given after a choice is made.

Laboratory experiments are susceptible to low incentives and therefore to unrealistic results regarding measurement of behavioural aspects. The approach taken here is that subjects are presented with simple WTP or choice tasks and are incentivised with monetary rewards that depend on their “performance” in the experiments. That is, participants are paid for real-stake lotteries in the experiments that follow.

Full details on the incentivisation of participants and on the allocation of participants’ payments are presented in Sections 3.2.3 and 4.2.3.

2.2.0.2 Surveys

We enhance the accuracy of experimental results by combining them with survey data. In general, data produced by experiments in a controlled fashion is considered more reliable, mainly because of incentivised elicitation design. Survey data, on the other hand, might amplify the effects of misunderstanding of questions and allow for various types of the response bias, like information recalling or alignment with socially acceptable answers. Experiments are considered free from such measurement errors and are also immune to other biases present in self-reported statements, e.g. as is observed when people respond differently to hypothetical than to real situations, or when they reply as if they were another person [109].

A question that follows naturally is whether behaviour that is observed in experiment tasks is correlated with self-assessment statements about willingness to take risks or

2.2 Economics and Behaviour

with self-reported replies to survey questions. A study which gives strong evidence supporting the validity of survey results is [52], in which risk attitudes are accurately depicted both by survey data and experimental input. In this sense, elicitation of risk attitudes via lottery-type questions and survey data can complement each other.

Except for typical demographic questions, we use surveys to convey to participants questions in an information security *context*. For example, we present participants with threat scenarios, alternative security measures and hypothetical situations in which they are asked to make choices.

2.2.1 Decision-making Models of Risk Behaviour

A short review of the theory and development of economic models of decision-making is provided in this section.

In developing a model for decision-making, there are three possible approaches to follow, as noted by Bell, Raiffa, and Tversky in [27]: “*First is descriptive, which is concerned with how and why people think and act the way they do. Second is normative, which is empirical in nature and deals with an idealized super rational intelligent person who thinks and acts as they should. Third, prescriptive studies such as subjective expected utility tell us what an individual should do and offer a great deal of pragmatic value.*”

Expected utility theory is the standard theory of individual decision-making under risk and uncertainty in Economics. After three decades of research on this subject, and especially on the direction of connecting experimental observations and theory, there have been quite a few models developed. The von Neuman-Morgenstern axiomatisation of Expected Utility [155] approached the decision-making questions from a normative (idealised decision-maker, the homo economicus) and prescriptive (practical directions for choices) view. A common formalisation is the notion of a *prospect* or *lottery* or *gamble*, which is “a list of consequences with associated probabilities”. More precisely, a *prospect* q is represented by a probability distribution $p = (p_1, p_2, \dots, p_n)$ over a set of corresponding outcomes $X = (x_1, x_2, \dots, x_n)$ which are exhaustive and mutually exclusive. Therefore, prospects or lotteries can be formalised in the following manner: if the consequence (outcome) q has an assigned probability p , then the alternative outcome r would occur with probability $1 - p$ and the lottery can be formalised as $(q, p; r, 1 - p)$. Formalisation is similar for any number of finite outcomes. The alternative options that the decision maker faces depend on uncertain factors and can produce different consequences. These uncertain factors are called *events*, or *states of nature* or *states of the world* (in Arrow [18], an event consists of all states of nature which satisfy some given condition). The mappings from the states of nature to the consequences are called *acts*. It is practical, for the purposes of decision-making, to consider a finite amount of

2.2 Economics and Behaviour

possible states that completely determine a finite amount of consequences. If the consequences are ordered then they can be considered as utilities that the decision-maker has to choose from or maximise. This is the “rational model of choice under uncertainty” [18] and it can be assumed that the individual can assign subjective probabilities in each state of nature.

In the various models, there is a distinction, originally established by Knight [94, 93], between *risk*, in which outcomes and probabilities of lotteries are known, and *uncertainty*, where at least some of the outcomes or probabilities are unknown. Another possible distinction is between *risky* and *riskless* choices. Risky decisions consist of lotteries, i.e. outcomes with assigned probabilities, whereas riskless decisions have to do with the acceptability of transactions (in which “goods and services are exchanged for money of labour” [91]). This is the choice situation that can be considered along risk and uncertainty, the, so to say, trivial situation of choice under certainty. These three alternatives in individual decision making create a partition of decision-making models.

Table 2.1: Properties of the Expected Utility Hypothesis

(1a) Completeness: $\forall q, r : q \succeq r$ or $r \succeq q$ or both.	
(1b) Transitivity: $\forall q, r, s : \text{if } q \succeq r \text{ and } r \succeq s, \text{ then } q \succeq s.$	
(1a) and (1b) \Rightarrow	(1) Ordering (2) Continuity: $\forall q, r, s : \text{if } q \succeq r \text{ and } r \succeq s, \text{ then } \exists p : (q, p; s, 1 - p) \sim r.$ (3) Independence: $\forall q, r, s : \text{if } q \succeq r \text{ then } (q, p; s, 1 - p) \succeq (r, p; s, 1 - p).$
(1) and (2) \Rightarrow	(4) \exists representation by a $V(\cdot) \in R : V(q) \geq V(r) \Leftrightarrow q \succeq r.$
(1) and (2) and (3) \Rightarrow	(5) \exists representation by a $V(q) = \sum p_i u(x_i), i = 1, \dots, n.$

The expected utility hypothesis is derived from three axioms (properties): *Ordering*, *Continuity* and *Independence*. Ordering consists of *Completeness* and *Transitivity*. Ordering and *Continuity* allow preferences over prospects to be represented by a real number produced by a function $V(\cdot)$. Independence along with function $V(\cdot)$ allow preferences over prospects to be represented in a form: $V(q) = \sum p_i u(x_i), i = 1, \dots, n$, where x_i are the potential outcomes of the lottery, $u(\cdot)$ is the subjective utility that the decision-maker evaluates the outcomes with, and p_i are the probabilities assigned to these outcomes. *Strict* and *weak* preferences are symbolised by “ \succ ” and “ \succeq ” respectively, whereas indifference between two prospects q and r is true when $q \succeq r$, and $r \succeq q$ and is symbolised by “ \sim ”. The aforementioned attributes are presented in Table 2.1:

We say that a prospect q , “first-order stochastically dominates” prospect r , if $\sum q_i u(x_i) \geq \sum r_i u(x_i)$.

Monotonicity is the property where first-order stochastically dominating prospects are

2.2 Economics and Behaviour

always preferred to the dominated ones, and it is accepted in either normative or descriptive models.

In particular, regarding the third property, (i.e. the “independence axiom”), systematic, (i.e. predictable), violations have been experimentally observed, such as the common consequence and the common ratio effects, shown by Maurice Allais [9]. A useful tool for the study and visualisation of the independence property has been the “Machina Triangle” [105], which is described in more detail in Section 2.2.1.2. The triangle-tool visualises the indifference curves of the decision-maker’s preferences. The slope of the curves reflects the risk-attitude of the individual: the more risk-averse the individual is, the steeper the curves are. Moreover, expected utility theory assumes “curves” with upward slopes which are linear and parallel to each other. Different models are produced by the relaxation of the parallel property and of the assumption of linearity. A particular form of relaxation of the independence axiom is called *betweenness*, which corresponds to the linearity of the indifference curves. Betweenness is defined in the following way: if $q \succ r$ then $q \succ (q, p; r, (1 - p)) \succ r$, $\forall p : 0 < p < 1$, where strict preference “ \succ ” can be translated as “preferred to”.

Models which are not based on objective probabilities, but on monotonic transformations of probabilities, such as decision weights $\pi(p_i)$, are a known case where betweenness does not hold.

The set of decision-making theories can also be divided into *conventional* and *non-conventional*. Conventional theories preserve the use of a function $V(\cdot)$ in order to describe individual preferences and, although they allow for the violation of the independence axiom, they maintain monotonicity. Conventional theories also assume “procedure and descriptive invariance”, i.e. they assume independence between preferences and the method used to elicit the preferences. An elicitation method can even be the way by which alternative options are described; this is usually called a “framing effect”. A particular observation of procedure invariance failure is “preference reversal” [99] when, for example, the procedure changes from “selling” to “valuating”. This failure might be interpreted by the invocation of different mental processes which elicit different orderings of the prospects, in other words, there is no unique ordering. At the same time, failure of procedure invariance means violation of the property of transitivity. Models which try to predict failure of procedure invariance and framing effects are not able to describe preferences with a single function $V(\cdot)$.

Another common assumption made in expected utility theory models, is that the preferences are elicited from stable traits of behaviour that the individual possesses. Self-perception theory [28], on the other hand, states that the individual creates its own behaviour by observing its previous actions, as an outside observer would (indicatively, [97]). This notion is related to, but still different from, attempts made to produce pro-

2.2 Economics and Behaviour

cedural models which describe a number of choice-heuristics that the decision-maker possesses and uses in an adaptive way [118], and consequently “decides how to decide”. The initial paper of Kahneman and Tversky on prospect theory [90] includes such heuristic-rules that the decision-maker uses during the first stage of the decision-making process.

Experimental evidence on lotteries have revealed overestimation of small probabilities and underestimation of more common events [40, 90]. This subjectivity in weighting objective probabilities gave rise to the aforementioned decision weighting models. An attribute of a preference function which depends on a probability weighting function π and on a utility u , is that it does not generally satisfy monotonicity. To cope with this consequence, the idea of rank-dependent expected utility was introduced [121, 122]. In rank-dependent utility models outcomes x_i are ordered from worse to best, and weighting depends on the relative position of the outcome in the ordered list, that is, weighting is a monotonic function normalised on the space $(0, 1)$. Intuitively, probability weighting functions express the way individuals subjectively distort a probability (psychophysics of risk) and they can explain the observed overestimation of small probabilities in gains (risk-seeking, e.g. lottery buying) and in losses (risk-aversion, e.g. insurance purchasing). Axiomatisation of rank-dependent models focuses on a weakened form of the independence property, the *comonotonic* independence (the name derived from common independence) which asserts that normal independence is preserved as long as there are no hedging effects in the outcomes ([33], Ch. 10.3.2.1). The usual independence requirement of Table 2.1 which should hold when we substitute outcome x in some prospect with outcome y , does not, generally, hold for rank-dependent models, because the substitution might change the ranking of the decision weights, and therefore might change the preference order. *Ordinal* independence allows substitution in lotteries which have common tails of events. The common tail is the one that can be substituted between lotteries without changing them, and is required in rank-dependent models.

The endowment effect [88, 96, 146] is the situation in which individuals find it difficult to depart from assets. Kahneman and Tversky [151] used the idea of a reference state, which corresponds to the current state and is usually preferred to be maintained by individuals, similarly to the endowment effect. Prospect theory assembles many of the pre-mentioned attributes. There are two domains defined by the reference point (current status): the domain of losses and the one of gains. Concavity of the gains domain is mirrored by convexity in the losses domain (the reflection effect) and this is in accordance with observed risk-averse behaviour regarding gains and a risk-seekingness regarding losses (see Figure 2.1). Moreover, the preference for avoiding losses is stronger than the preference to acquiring gains (loss-aversion), by a roughly estimated factor of two. Considering high and low probabilities and the domains of gains and losses, we

2.2 Economics and Behaviour

can construct the four-fold pattern of risk attitude (FFP) (see Table 2.2) [87]. This construction describes four possible pairs: high- and low-probability in both gains and losses, and is very useful in analysing the corresponding behaviour. It is not known whether the FFP holds for all decision-making contexts, or whether the manifestation of the pattern depends on the decision elicitation process [74].

In the original paper on prospect theory [90], an editing phase was assumed, during which the decision-maker coded the outcomes as gains or losses. In the extension of the theory, cumulative prospect theory (CPT) [152], a rank-dependent approach was followed and decision weights were used in this context, making the coding phase obsolete and the theory more concrete. The advantage of using the cumulative decision-weights is that we can have a transitive preference function that is monotonic, thus allowing for stochastic dominant preferences. Another important property is that we can use different weighting functions for the positive and the negative outcomes (sign-dependence). Subsequently, cumulative prospect theory moves away from the procedural approach, i.e. the editing/coding phase, where a number decision rules are applied (this is also found in Payne's model [118]) and gets closer to the realm of conventional models, providing a single preference function. Prospect theory works on risky prospects, but can be extended to uncertain prospects as well [153].

A combination of loss aversion and a parameter of how frequently an investment is evaluated, produced the notion of *myopic loss aversion* [29], setting a context of decision-makers with "short horizons and a strong distaste for losses" [147]. Myopia is a special form of framing, which allows the decision-maker to only consider some parts of the prospects more frequently and is similar to Kahneman's and Tversky's isolation effect.

Another category of models are the ones related to regret and disappointment theory [26, 102]. According to this theory, the individual compares the possible outcomes of a specific lottery. In the decision-making case, each possible choice produces an outcome which can be compared to alternatives that "might have been". This way, the decision-maker estimates his/her expected disappointment. The main property of regret theory is that it does not require transitivity. Another important point is that lotteries are considered statistically independent and therefore their outcomes are uncorrelated (this is equivalent to the so-called weighted-utility theory). The idea of regret-aversion [102] sketches the fact that the existence of large differences between an outcome and its possible alternatives leads to very large regrets. Regret-aversion allows for the violation of transitivity by producing a cycle of preferences, but it also allows for the violation of monotonicity, and in this sense can be categorised as a non-conventional theory.

Starmer [143] highlights three distinct attributes which have been experimentally observed and should be incorporated in any conventional model for decision-making that

2.2 Economics and Behaviour

can be tested with a Machina triangle (see Section 2.2.1.2 for more details). Namely:

- generalised fanning-out of indifference curves should not be assumed,
- betweenness should also not be assumed, i.e. indifferent curves should not be considered linear,
- it should be taken into consideration that the behaviour of the probabilities inside the triangle is more closely related to expected utility theory than the behaviour on the borders of the triangle (i.e. where extreme probabilities, whether very small or very large, dwell) which tend to cause the violations.

A rough conclusion from field evidence is that probability weighting functions with inverse s-shaped probability transformations (e.g. as in Figures 2.2 and 2.3) tend to fit the observed data better. Given that there are many ways to describe such weighting functions, a question that emerges is how many parameters should be used in the models. Indeed, there have been many different approaches [98, 70] which take advantage either of the simplicity of a one-parameter-function or of the flexibility of a function with two parameters.

Dynamic choice is a more complex framework for decision-making. In such models we consider decision nodes which depend on events and the decision-maker chooses the appropriate paths of a choice tree. There are issues of dynamic consistency, but dynamic choices can be consistent with rank-dependent models [131].

Finally, consequentialism is an assumption which states that a choice of a decision node is made independently of risks foregone in the past and also of decisions which cannot be reached via the decision tree. Intuitively this is a very strong assumption which might not hold for many real-world decision-making environments, including information security.

To conclude this short review, we highlight prospect theory and its cumulative version. There is strong evidence that predictions of this theory align with many empirical observations, and thus the theory can provide a tool for analysing behaviour of decision-makers either under risk or uncertainty. ²

In this short review we have described the main attributes which pertain economic models relating to decision-making. More specific experimental studies which relate to information security are presented in Section 2.1.4. In the following sections we describe the main theories we use in evaluating and explaining various experiment results of this study.

²It is worth mentioning the existence of a formal proof for prospect theory, through an additive conjoint measurement model [95].

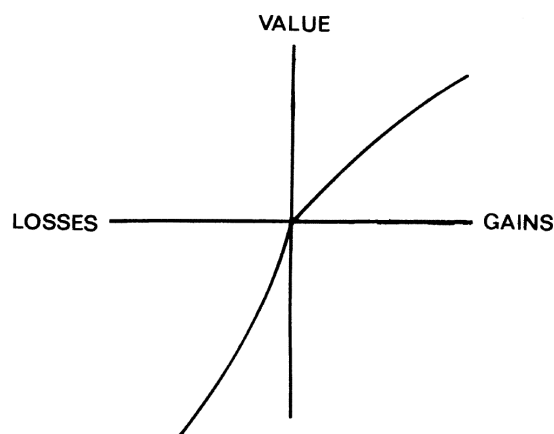
2.2 Economics and Behaviour

2.2.1.1 Prospect Theory

We use prospect theory in order to explain various observed behavioural traits of security professionals and potential violations of expected value maximisation. The details and the main characteristics of the theory are presented in this section.

The original version of the theory, prospect theory (PT) was presented by Kahneman and Tversky in 1979 [90]. Cumulative prospect theory (CPT) was presented in 1992 as an advancement [152]. The initial theory assumes there is a value function v which represents the valuation of monetary outcomes by the individual, i.e. the psychological impact of outcomes to individuals. This value function is the equivalent of the traditional utility function, although Kahneman and Tversky never used the word “utility”, probably in order to make a clear diversification from expected utility theory (EUT).

Figure 2.1: Prospect theory’s hypothetical value function.



The theory also assumes a weighting function w that distorts the probability p_i of each event i . Function w describes risk attitude towards probabilities of outcomes. An important point is that prospect theory, similarly to other non-expected utility theories, uses a non-linear weighting function. It is shown that expected utility theory fits observations reasonably well, in the case of linear moderate probabilities, but not when sufficiently small or sufficiently large probabilities are involved [40]. In Figures 2.2 and 2.3 the estimated weighting function w is shown for the domains of gains and losses respectively (images taken from [152]):

The certain monetary amount c for which an individual becomes indifferent between a risky choice and c , is called *certainty equivalent*. The estimation of the transformations is elicited by the medians of c/x plotted against probability p , where x is the maximum lottery outcome (either a gain or a loss) and c is the certainty equivalent. In Figure 2.3, c represents the certainty equivalents subjects chose in order to avoid a lottery of the form $(x, p; 0, 1 - p)$; this amount is divided by the corresponding non-zero outcome x on

2.2 Economics and Behaviour

Figure 2.2: Risk attitude for gains: ratio c/x by the probability of gain.

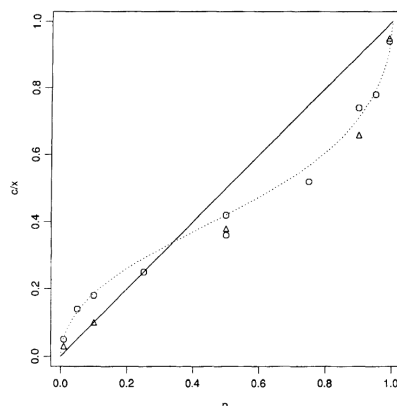
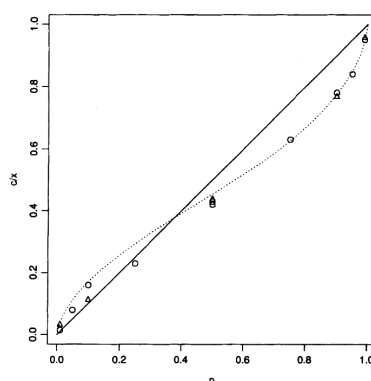


Figure 2.3: Risk attitude for losses: ratio c/x by the probability of loss.



the vertical axis. In particular, the part of the curve that lies above the diagonal $y = x$ denotes risk aversion as the individual accepts to lose a larger c/x ratio than the actual probability of loss. Whereas, the part of the curve beneath $y = x$ indicates risk seeking behaviour as the probability of loss is larger than the ratio that the decision-maker is willing to give away, i.e. the individual takes the risk.

In CPT, f is called an uncertain prospect (or act), and is a function from the set of all states S to the set of all consequences X , $f : S \rightarrow X :: s \rightarrow x$.

Considering a partition (A_i) of the states of the world S , a prospect (act) f is represented by a sequence of pairs of the form (x_i, A_i) , where x_i is the ordered outcome, in case that the corresponding event A_i occurs. The notion of capacity is used by Choquet in [44]. A capacity W is a non-additive set function, such that it maps subsets A of S to real numbers, $W : S \rightarrow \mathbb{R} :: A \rightarrow \kappa$. Additionally, $W(\emptyset) = 0$ and $W(S) = 1$ and $\forall A, B$ subsets of $S : B \subset A \Rightarrow W(B) \leq W(A)$.

Capacities are considered separately for positive and negative prospects, that is, prospects with only positive or only negative outcomes. Mixed prospects f are possible, as we consider the positive f^+ or the negative f^- part of each prospect: for example,

2.2 Economics and Behaviour

$f^+(s) = f(s)$, if $f(s) > 0$ and $f^+(s) = 0$, if $f(s) \leq 0$ for the positive part of a prospect and similarly for the negative part. Decision weights π_i are defined for the positive (gains) and the negative (losses) domain as:

$$\pi_n^+ = W^+(A_n) \text{ and } \pi_i^+ = W^+(A_i \cup \dots \cup A_n) - W^+(A_{i+1} \cup \dots \cup A_n), \text{ for } 0 \leq i \leq n-1.$$

$$\pi_{-m}^- = W^-(A_{-m}) \text{ and } \pi_i^- = W^-(A_{-m} \cup \dots \cup A_i) - W^-(A_{-m} \cup \dots \cup A_{i-1}), \text{ for } -m \leq i \leq 0.$$

The value function v is defined from the set of outcomes X to the real numbers, $v : X \rightarrow \mathbb{R}$, $v(x_0) = 0$ and v is strictly increasing. So, by CPT there is a function V , such that: the valuation of the positive prospects is $V(f^+) = \sum \pi_i^+ v(x_i)$ and the valuation of the negative prospects is $V(f^-) = \sum \pi_i^- v(x_i)$. Finally, the total valuation is the sum of the positive and the negative one: $V(f) = V(f^+) + V(f^-)$. The difference between the two versions of prospect theory is that in the cumulative version, the weighting function w that transforms probabilities is rank-dependent, i.e. the outcomes of the lotteries have to be ordered, and the weights, which are for simplicity formalised as $w(p_i)$, depend on the ranking position of the corresponding outcomes. In fact, as the name implies, it is the cumulative probabilities which correspond to the outcomes that are subject to the weighting transformations. The main reason for this modification was that the initial prospect theory failed to maintain stochastic dominance. Moreover, CPT expands to many-outcome prospects.

A variety of experiments reveal a particular phenomenon, called the four-fold pattern (FFP) of risk behaviour [87]. The FFP describes the suspected non-linear transformation of probabilities and the attitude towards loss aversion. The phenomenon categorises risk behaviour into risk-seeking or risk-averse, depending on the magnitude of the probability and the domain (gains or losses) of the lottery. A visualisation of the FFP elicited from the sets of lotteries $(0.95, \pm 10,000; 0.05, 0)$ and $(0.05, \pm 10,000; 0.95, 0)$ is shown in Table 2.2 (adapted from [87]).

Table 2.2: The Four-fold Pattern of Risk Attitude

	Gains	Losses
High Probability (Certainty Effect)	95% chance to win \$10,000 Fear of disappointment RISK AVERSE Accept unfavourable settlement	95% chance to lose \$10,000 Hope to avoid loss RISK SEEKING Reject favourable settlement
Low Probability (Possibility Effect)	5% chance to win \$10,000 Hope of large gain RISK SEEKING Reject favourable settlement	5% chance to lose \$10,000 Fear of large loss RISK AVERSE Accept unfavourable settlement

2.2 Economics and Behaviour

The most unexpected result of prospect theory is the risk-seeking behaviour for high probability losses. It is not known whether, or how, the FFP is manifested in various contexts. We discover this pattern, for the domain of losses, in various instances of the experiments that follow. It is noteworthy that there are boundaries which allow for the manifestation of the phenomenon. For example, probability weights $w(p_i)$ have to be relatively large compared to outcome valuations $v(x_i)$, i.e. the overweighting for small and the underweighting for large probabilities has to be sufficiently large in order to overcome the effects caused by the valuation function v [74]. This means, that the FFP might be underlying in a decision-making process, but there is a possibility that it is not sufficiently intense to be detected. The experimental settings in which we detect the FFP are presented in detail in Chapters 3 and 4.

2.2.1.2 The Machina Triangle

A very useful instrument for visualising preferences amongst lotteries is the “probability triangle” also called “Machina triangle”. We use this instrument as the basis of the proposed decision-making model for information security investment which is presented in Section 2.2.2.

Interestingly, the instrument was presented originally by Marschak [108] and later by Machina [104], and has been widely used in the economics literature. The instrument requires that the outcomes of choice alternatives are ordered in increasing order, whether they are in the domain of gains or losses. Then, in the case of three outcomes, for example, $x_1 < x_2 < x_3$, we have a corresponding triplet (p_1, p_2, p_3) , where p_i is the probability of occurrence of outcome x_i . We can plot probability p_1 against probability p_3 , and the remaining probability p_2 is: $p_2 = 1 - p_1 - p_3$ ³. Assuming that the individual decision-maker possesses a utility function u , from the set of outcomes to the real numbers, $u : X \rightarrow \mathbb{R}$, then, the solutions of the equation:

$$\sum u(x_i)p_i = u(x_1)p_1 + u(x_2)(1 - p_1 - p_3) + u(x_3)p_3 = \text{constant} \quad (2.1)$$

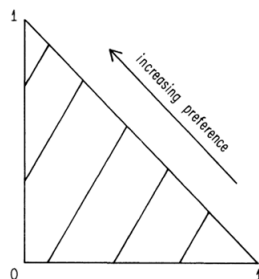
depict the risk attitude of the individual, as they reveal the points in the triangle that are indifferent to the decision-maker (i.e. they have the same expected utility). These lines are called indifference curves and are depicted in Figure 2.4 (image taken from [105]).

The slope of the indifference curves can be calculated to be $\lambda = \frac{[u(x_2)u(x_1)]}{[u(x_3) - u(x_2)]}$.

³The instrument setting concerns an objective perception of probabilities; experimentally elicited subjective preferences are presented in Figure 2.7.

2.2 Economics and Behaviour

Figure 2.4: Indifference curves in the “Machina Triangle”



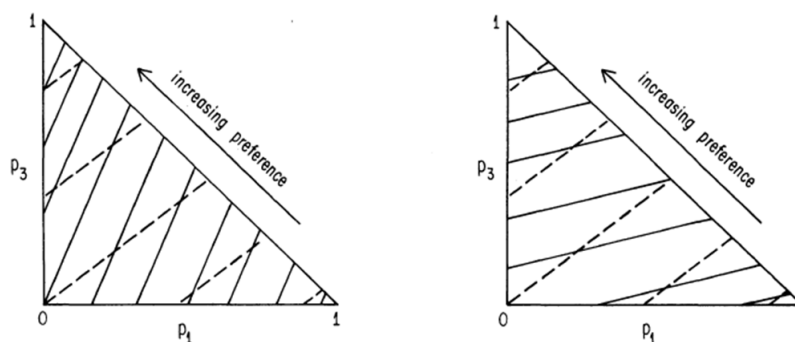
In the case of omitting the utility function:

$$\sum x_i p_i = x_1 p_1 + x_2(1 - p_1 - p_3) + x_3 p_3 = \text{constant}, \quad (2.2)$$

the graphical result is a family of curves (here lines) called iso-expected value lines.

A comparison between the iso-expected lines and the indifference curves reveals the risk attitude of the decision-maker. In particular, if the indifference curves are steeper than the iso-expected lines, then the individual shows risk aversion, whereas in the opposite case the decision-maker is risk seeking. In Figure 2.5 iso-expected lines are depicted with dashed lines and indifference curves are the solid lines (image taken from [105]).

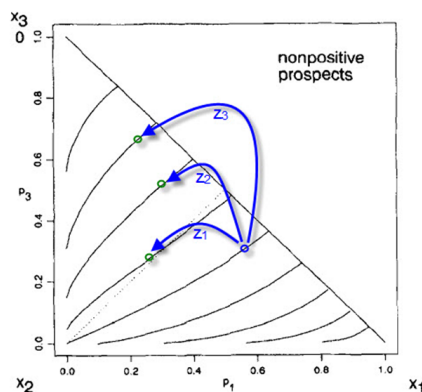
Figure 2.5: Iso-expected lines and indifference curves



Since the decision-maker has an incentive to move from a point of larger potential losses to a point of smaller losses, the “movements” in the triangle which give stochastically dominating lotteries and are therefore preferable, are the ones with North-West direction. The opposite is true for South-East movements. In this framework, we can define information security investment as monetary amounts, say z_i , that need to be spend for conducting a “movement” or “jump” from the current point in the Machina triangle to a more preferable one. This “jump” has a cost, and the cost can be exactly specified by the difference between the expected utility of the initial point and the destination point, as depicted in Figure 2.6, which has been adapted from [152] (a formal representation of this idea is presented in Section 2.2.2).

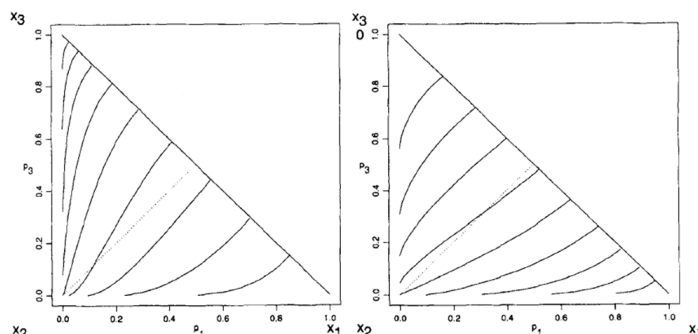
2.2 Economics and Behaviour

Figure 2.6: Investment for achieving a more preferable state



Considering the information security environment, it is not necessary to separate between physical, technical and administrative measures, as they can all be considered as indistinguishable controls deployed by the act of investing. The elicitation of the indifference curves, however, is not a trivial task. As stated in Section 2.2.1.1, indifference curves can be the product of a value function v and a weight function w . The form of such curves has been investigated by Kahneman and Tversky for gains and losses separately (see Figure 2.7; diagrams taken from [152]).

Figure 2.7: Indifference curves for the domain of gains (left) and losses (right)



In the spirit of the review of Section 2.2.1, it is noteworthy that an approach presented by Machina and Scmeidler [106] assumes that decision-makers have probabilistic beliefs, without needing to be utility maximisers. This is in contrast to one of the most influential interpretations of probabilities, i.e. the subjective interpretation of Savage [132], which requires both assumptions.

For the purposes of this study, however, the important point is the notion that the probabilistic *beliefs* of the decision-maker can be represented by the decision-maker's subjective probabilities, which, in turn, correspond to the decision-maker's risk preferences.

2.2 Economics and Behaviour

2.2.1.3 Saliency Theory

We use this theory in order to examine the behaviour of information security professionals with respect to their risk attitude towards worst-case outcomes. The reader can find a detailed description of the theory in this section.

Saliency theory [32] states that it is the saliency of outcomes, instead of the probabilities, which attract the focus of the decision-maker. Saliency is the phenomenon in which “when one’s attention is differentially directed to one portion of the environment rather than to others, the information contained in that portion will receive disproportionate weighting in subsequent judgements” ([145]). For example, suppose that an information security professional has to choose between two security measures. The professional’s attention might be focused on the attributes of these security products which differ the most, ignoring the other attributes.

Worst-case is a frequently used term in this study and it can be considered as an unusual case: “our mind has a useful capability to focus on whatever is odd, different or unusual” ([87]). Saliency is formalised by ordering and diminishing sensitivity, and is therefore in accordance with rank-dependent models of choice, and cumulative prospect theory in particular. Context is expressed by diminishing sensitivity relevantly to status quo: “The role of context is captured by diminishing sensitivity (and reflection): the intensity with which payoffs in a state are perceived increases as the state’s payoffs approach the status quo of zero, which is our measure of context” ([32], p.16). There are two differences between saliency theory and classic rank-dependent models [122, 152]:

- Overweighting depends on the ranking of the outcomes, but it also depends on their magnitude.
- The worst possible outcome might not have enough difference from the rest of the choice context in order to be salient and therefore could be underweighted instead of overweighted. This means that with this model, worst-case is salient only if the difference between the worst-case and the rest of the choices is “sufficiently” large.

We use saliency theory in our experimental design of Chapter 3 to examine whether ranking of lottery outcomes (or payoffs), as well as outcome-magnitude, influence decisions of information security professionals. Local thinking is another term related to disproportionate focus on some outcomes. Local thinking is defined as the phenomenon in which decision makers do not consider all information available to them, but tend to overemphasise the information their mind focuses on [67].

The set of the states of the world is S and we can choose between two lotteries, L_i ,

2.2 Economics and Behaviour

$i = 1, 2$, with risky prospects, which have corresponding minimum and maximum outcomes x_s^{min} and x_s^{max} , respectively, for each lottery i in each state s . The probabilities that correspond to each state are exhaustive and mutually exclusive. Saliency function σ is a continuous and bounded function with the following three properties ([32], p.7):

1. Ordering: for states s and $\bar{s} \in S$,

$$\text{if } [x_s^{min}, x_s^{max}] \subseteq [x_{\bar{s}}^{min}, x_{\bar{s}}^{max}], \text{ then } \sigma(x_s^i, x_s^{-i}) < \sigma(x_{\bar{s}}^i, x_{\bar{s}}^{-i}). \quad (2.3)$$

where $x_s = (x_s^i)_{i=1,2}$ are the payoff vectors for state s , for lotteries 1 and 2.

(x_s^{-i} denotes the payoff in state s for lottery j , so that $j \neq i$).

Finally, x_s^{min} and x_s^{max} are the smallest and largest payoffs in x_s .

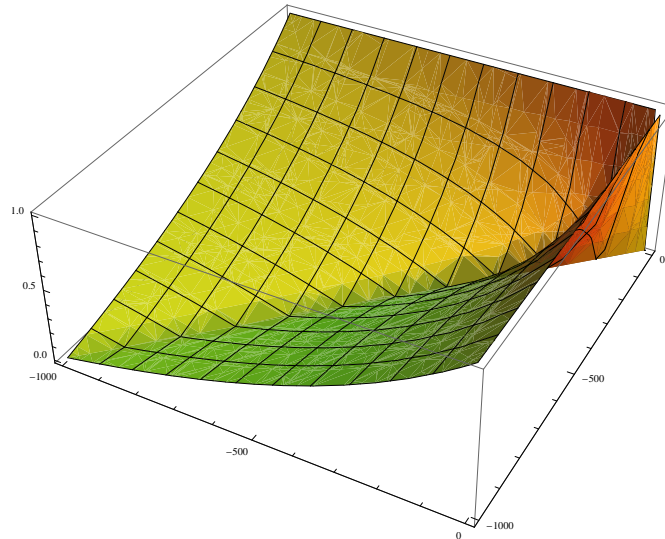
2. Diminishing sensitivity: if $x_s^i > 0$, for $i = 1, 2$ then $\forall \epsilon > 0$,

$$\sigma(x_s^i + \epsilon, x_s^{-i} + \epsilon) < \sigma(x_s^i, x_s^{-i}). \quad (2.4)$$

3. Reflection: for any two states s and $\bar{s} \in S$, with $x_s^i, x_{\bar{s}}^i > 0$, for $i = 1, 2$:

$$\sigma(x_s^i, x_s^{-i}) < \sigma(x_{\bar{s}}^i, x_{\bar{s}}^{-i}) \text{ if and only if } \sigma(-x_s^i, -x_s^{-i}) < \sigma(-x_{\bar{s}}^i, -x_{\bar{s}}^{-i}). \quad (2.5)$$

Figure 2.8: Values of saliency function $\sigma(x, y) = \frac{|x-y|}{|x|+|y|}$, for $x \in (-1000, 0)$ and $y \in (-1000, 0)$.



A visual representation of the values of a simplified saliency function is presented in Figure 2.8. The extreme values of the representation are 0 and -1000 , because these are the values used in the experiment tasks that follow. We observe that higher values

2.2 Economics and Behaviour

occur for the variable pair values $(x, y) = (-1000, 0)$ and $(x, y) = (0, -1000)$, whereas the function takes zero values for $x = y$.

The methodology for calculating salience theory-predicted preferences over two lotteries can be summarised in the following steps. The Mathematica [2] code for executing these steps for the purposes of Experiment 1 (see Chapter 3) can be found in Appendix A.1.12.

- Step 1: write all possible state space pairs by combining all outcomes from the first and the second lottery.
- Step 2: rank all pairs by their salience σ :

$$\sigma(x_s^i, x_s^{-i}) = \frac{|x_s^i - x_s^{-i}|}{|x_s^i| + |x_s^{-i}| + \theta}. \quad (2.6)$$

Note that a salience function serves as the connecting link between the cognitive notion of salience and the properties of ordering, diminishing sensitivity and reflection. Thus, any function which maintains these properties is eligible. The vector containing the payoffs of the lotteries in state s is $x_s = (x_s^i)_{i=1,2}$ and x_s^{-i} is the state s -outcome of lottery L_j , where $j \neq i$. Parameter θ is estimated as $\theta = 0.1$ ([32], page 24).⁴

- Step 3: assign a number k to each pair, starting from the most salient pair. For example, the most salient pair across all states $\sigma(x_s^{max}, x_s^{min})$ has $k = 1$.
- Step 4: compute the sum:

$$\sum_{s \in S} \delta^{k_s} \pi_s [v(x_s^1) - v(x_s^2)], \quad (2.7)$$

where, π_s is the smallest probability of the two outcomes of the pair. Note that the utility function $v(\cdot)$ has to be linear, for calculating the differences $v(x^1) - v(x^2)$. For example, for two lotteries L_i and L_j , we have $L_i \succ L_j$ if and only if the sum (2.7) is positive. An important part of the calculation is the value of $\delta \in (0, 1]$, which expresses the degree of local thinking for a decision-maker. For $\delta = 1$, the decision-maker's probability weighting is exactly the objective probabilities. For $\delta < 1$, local thinking favours the first lottery, L_i , when it "pays more" in the more salient lottery states. The salient states are the ones that are less discounted by δ due to the exponent k . In our case, only negative outcomes are considered, so $\delta < 1$ favours L_i when it has smaller losses in the most salient states⁵.

⁴Note that outcomes are presented to belong to the same state s here; however, we can allow for all possible combinations of state comparisons, as is explained in detail in Chapter 3.

⁵It is noteworthy that δ has been estimated as $\delta = 0.7$ and that for $\delta = 0.73$ the Allais Paradox is explained by the narrow framing of the local thinker.

2.2 Economics and Behaviour

2.2.1.4 Uncertainty and Ambiguity

This section provides further details on the notions of *uncertainty* and *ambiguity* that are frequently used throughout the study.

In the initial approach of Knight in 1921 [93], risk and uncertainty are two separate things, with risk being “a quantity susceptible of measurement”, whereas uncertainty being “immeasurable risk”. During the same year as Knight’s publication, Keynes [92] studied the type of uncertainty that has to do with the outcome of an event, e.g. whether something will be successful or not. In the context of Ellsberg’s work [55] uncertainty or ambiguity has to do with the success probability itself, i.e. in this terms “ambiguity is the uncertainty about probabilities”. In many cases, ambiguity is considered as a special case of uncertainty which focuses on probability estimation. In contrast, the term “uncertainty” is used more loosely and generally in decision-making. Einhorn and Hogarth [54] define ambiguity as the “intermediate state between ignorance and risk”. In this research *ambiguity* denotes a range of lottery probabilities or a range of outcomes, in contrast to *risk* which defines specific lottery probabilities and outcomes.

Uncertainty does not involve complete information about the states of nature, as is described in the Ellsberg paradox [55]. The experimental setting of the “paradox” presents two pairs of gambles to the decision-makers to choose from:

“There are exactly 30 red and also 60 black and yellow balls in an unknown ratio in an urn”. The first question regards which of the two gambles is more preferable:

- Gamble A: “win 100\$ if you draw a red”.
- Gamble B: “win 100\$ if you draw a black”.

The second question concerns the preference between two other gambles:

- Gamble C: “win 100\$ if you draw a red or yellow”.
- Gamble D: “win 100\$ if you draw a black or yellow”.

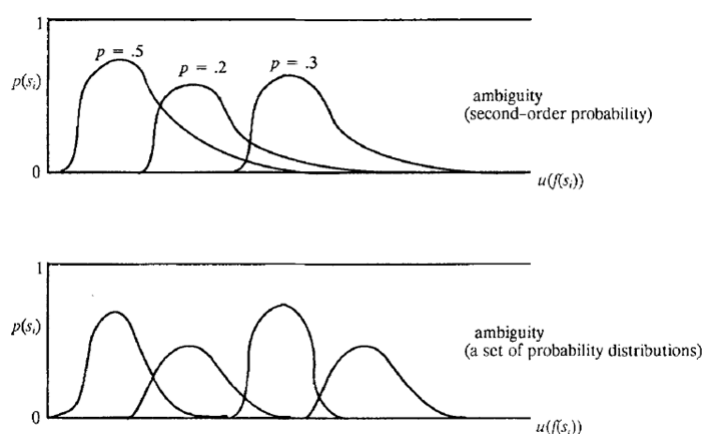
The majority of people systematically prefer Gamble A to B and Gamble D to C. This leads to the paradox of considering probability $P(\text{red}) > P(\text{black})$ in the first choice, whereas implying $P(\text{black}) > P(\text{red})$ in the second.

But, there can be different degrees of uncertainty of probability, namely two, as stated by Camerer and Weber in [39]. Assuming states s_i which correspond to outcomes (consequences) via an act $f(\cdot)$ and assuming a utility for each outcome, we can plot

2.2 Economics and Behaviour

the utility of the consequence of an act of each state $u(f(s_i))$ against its corresponding probability of occurrence. When the individual does not know the probability distribution which corresponds to each state, but he or she can assign a probability to each possible (conceivable) distribution, then we have the so-called uncertainty as second-order probability. In contrast, when the decision-maker is not in position to apply probabilities to distributions, uncertainty is the expression of a set of distributions. These two levels of uncertainty are depicted in Figure 2.9 (diagrams taken from [39]).

Figure 2.9: Levels of uncertainty.



In the event of not having available information regarding the occurrence of events, we deal with fully subjective models. In contrast, there can be some information available to the decision-maker, but not enough to shift the decision from uncertainty to risk. It is noteworthy that, in a different approach, some researchers favour the explicit characterisation of ambiguity as the amount of missing information [64].

Ambiguity can be represented similarly to risk (see Section 2.2.1). All possible and conceivable states are represented by the state space S . Elements $s \in S$ are the states of nature, and sets of elements $E \subset S$ are the events. We can denote a σ -algebra A of the events. Outcomes are represented as elements of the outcome space X . Acts are the mappings from S to X , over which the decision-makers reveal their preferences. Finally, the equivalent of a probability distribution in risky choices for uncertain and ambiguous choices is the notion of capacity, as introduced in Section 2.2.1.1.

2.2.2 Modelling Investment Decisions

A formalisation of investment decisions in information security is presented in this section, including two attributes: security and the operational posture of the system. The purpose of this formalisation is two-fold. On the one hand, it provides a proposed codification for information security investment. On the other hand, it assists the reader

2.2 Economics and Behaviour

in understanding certain experiment tests found in Chapters 3 and 4 by presenting the reasoning behind the tests, in a formal manner.

The starting assumption is that the “system” under protection⁶, with its broader sense, has a current state, the status quo, which consists of two main attributes: security (*SEC*) and operability (*OPS*). Operational advantages or disadvantages represent any kind of efficiency or deficiency in time, personnel, procedures and other resources that are needed for the completion of some business function. Such multiattribute utility models are proven to preserve certain advantages, e.g. utilities maintain their properties even if they are built on non-expected utility models, and specifically on rank-dependent models and prospect theory [114].

The probability space of each attribute is described by a simplex $\Delta = \Delta(n)$, where n expresses the number of specific probabilities associated with given outcomes, and $n \in \mathbb{N}$. Each state of nature can be represented by a risky prospect, i.e. a finite set of pairs of the form: (probability, outcome). Therefore, for example, for $\Delta(1)$ each attribute is described as $SEC = (p, x_1; 1 - p, x_2)$ and $OPS = (q, y_1; 1 - q, y_2)$ and the current state is (SEC, OPS) . For simplicity, we can have x_i and y_i fixed (e.g. equal to the value of the assets under protection) and describe the two attributes only by the pair of probabilities, e.g. for $\Delta(1)$: $SEC = (p, 1 - p)$ and $OPS = (q, 1 - q)$.

A shift from the current state to a new state is described by a function S such that:

$$S_n : \Delta(n) \times \Delta(n) \times \mathbb{R} \rightarrow \Delta(n) \times \Delta(n) \quad (2.8)$$

E.g. for $\Delta(1)$:

$$S_1 : \Delta(1) \times \Delta(1) \times \mathbb{R} \rightarrow \Delta(1) \times \Delta(1) :: ((p, 1 - p), (q, 1 - q), z) \mapsto ((p', 1 - p'), (q', 1 - q')) \quad (2.9)$$

where z is the monetary amount of security investment which allows for a new (more beneficial) state to be reached, so that:

$$S((SEC, OPS), z) = (SEC', OPS'). \quad (2.10)$$

E.g. for $\Delta(2)$:

$$S((p_1, p_2, 1 - p_1 - p_2), (q_1, q_2, 1 - q_1 - q_2), z) = ((p'_1, p'_2, 1 - p'_1 - p'_2), (q'_1, q'_2, 1 - q'_1 - q'_2)). \quad (2.11)$$

S is assumed non-injective and surjective, so that different states with different investment amounts can lead to the same security and operational posture and also all

⁶We use the term “system” in the spirit of [133], i.e. as a complex structure, that allows for interactions with other systems, bears emerging properties and can misbehave in certain ways (manifests “bugs”).

2.2 Economics and Behaviour

postures can be achieved by an appropriate amount. If $z > 0$ then $(p'_1, p'_2, 1 - p'_1 - p'_2)$ is expected to second-order stochastically dominate (SSD) $(p_1, p_2, 1 - p_1 - p_2)$ and $(q'_1, q'_2, 1 - q'_1 - q'_2)$ second-order statistically dominates (SSD) $(q_1, q_2, 1 - q_1 - q_2)$, but first-order stochastic dominance (FSD) is not required ⁷.

To make the investment scenarios more realistic, transition to the new state can occur with some probability r and the current state of nature can be maintained with probability $1 - r$.

Preferences on various states of the form (SEC, OPS) can be defined as a binary relation on the Cartesian product $A = \Delta \times \Delta$. The conditions for numerical representation of these preferences can be explored by conjoint measurement (CM) techniques [33]. Conjoint measurement theory studies binary relations defined on Cartesian products of sets. Such relations can be defined for various attributes and/or different states of nature between which the decision-maker has to state his/her preference. The theory sprang from mathematical psychology in an attempt to quantify psychological attitudes and utilities [103].

In general, for n -dimensional elements x and y on space A , an additive utility model is at the core of CM, and a preference relation \succeq (or \succ) is defined as:

$$a \succeq b \Leftrightarrow \sum_{i=1}^n u_i(a_i) \geq \sum_{i=1}^n u_i(b_i), \quad (2.12)$$

where utilities u_i are real-valued functions over the set A_i , and A is the finite product set $A = A_1 \times A_2 \times \dots \times A_n$, where n represents the number of attributes (in our case $n = 2$ and $A = A_1 \times A_2 = \Delta \times \Delta$).

The abstraction u_i , for our purposes, is the corresponding utility which values security level (u_1) and the utility that values operability (u_2). So, preference of position (state) a to position (state) b , is given by:

$$a \succeq b \Leftrightarrow u_1(p) + u_2(q) \geq u_1(p') + u_2(q'), \quad (2.13)$$

given that only probabilities are used to describe positions and that in $\Delta(1)$ probabilities p and q are enough to describe the positional prospect. The pair of security level and

⁷Lottery A has first-order stochastic dominance over lottery B , if A has at least as high a probability of receiving at least the same outcome (gain) as in the case of B ; and equivalently for losses. Lottery A has second-order stochastic dominance over lottery B , if B is a mean-preserving spread of A . An expected utility maximiser should always choose the dominant lottery.

2.2 Economics and Behaviour

operational capacity which represents the current state of the world is:

$$a = (SEC, OPS) = (p, q) = ((p; 1 - p), (q; 1 - q)) = ((p, x_1; 1 - p, x_2), (q, y_1; 1 - q, y_2)). \quad (2.14)$$

Preference between the two positions a and b ultimately means a preference amongst pairs of gambles:

$$a \succeq b \Leftrightarrow ((p, x_1; 1 - p, x_2), (q, y_1; 1 - q, y_2)) \succeq ((p', x_1; 1 - p', x_2), (q', y_1; 1 - q', y_2)). \quad (2.15)$$

There are three ways of constructing models of relations on a product set, as described by Bouyssou and Pirlot in [33]. One approach would be the combination of individual valuations of each alternative state for each attribute; and the preference relation would be defined by a real-valued function F on the product set $\prod ui(A_i)$:

$$a \succeq b \Leftrightarrow F(u_1(p), u_2(q), u_1(p'), u_2(q')) \geq 0. \quad (2.16)$$

In terms of cumulative prospect theory-“utility”, the preference relation can be presented as:

$$a \succeq b \Leftrightarrow \begin{aligned} & F(\pi(p) \cdot v(x_1) + \pi(1 - p) \cdot v(x_2), \\ & \pi(q) \cdot v(y_1) + \pi(1 - q) \cdot v(y_2), \\ & \pi(p') \cdot v(x_1) + \pi(1 - p') \cdot v(x_2), \\ & \pi(q') \cdot v(y_1) + \pi(1 - q') \cdot v(y_2)) \geq 0. \end{aligned} \quad (2.17)$$

This expression does not pre-assume any completeness or transitivity requirement.

A more realistic scenario would be to allow for non-fixed amounts of losses or gains to be included in the prospects. Namely, for security gains and losses $x = (x_1, \dots, x_{n+1})$ and operational outcomes $y = (y_1, \dots, y_{n+1})$, both being $(n + 1)$ -dimensional vectors of $X = X_1 \times \dots \times X_{n+1}$.

In this case and for $\Delta(1)$, the shift function can be defined as:

$$S_2 : (\Delta(1) \times X)^2 \times R \rightarrow (\Delta(1) \times X)^2 :: \quad (2.18)$$

$$((p, x_1; 1 - p, x_2), (q, y_1; 1 - q, y_2), z) \mapsto ((p', x'_1; 1 - p', x'_2), (q', y'_1; 1 - q', y'_2)).$$

S_1 and S_2 are the shift or “jump” functions that were depicted on a Machina triangle in Section 2.2.1.2 (Figure 2.6). S_1 and S_2 are useful in defining the positional shifts given an investment amount z . But, if the decision-maker has to choose between future alternative investment amounts, say z_1 and z_2 , then it would make sense to define a preference relation on (future) outcome triplets of the form $\sigma = (SEC, OPS, \zeta)$, with ζ representing the amount needed to be invested, in order to reach state σ . Expanding

2.3 Summary

on the pre-mentioned formalism, we can consider necessary investment amount ζ as a third attribute, so that preferences can be established on space $A = (\Delta \times X)^2 \times Z$, where $\zeta \in Z \subset \mathbb{R}$. This process is cognitively more natural, because it allows the decision-maker to directly compare future outcome postures of any investment in information security, including the investment amount.

There are two main tools for analysing the preference relations on additive value function models and on their generalised forms, namely, marginal preferences and marginal traces on levels. These tools are beyond the scope of this study and the interested reader can find more information in Appendix A.3.0.1. We do not pursue the aforementioned model any further; instead, we focus on eliciting risk attitudes of security professionals experimentally.

2.3 Summary

In this chapter we argued the importance of information security and the role of the security professional. We described the context of information security and risk management in order to convey to the reader the kind of decisions that professionals have to face. We discussed a number of risk behaviour patterns and biases that potentially influence these decisions.

We described the research methodology followed in this study for eliciting risk attitudes of individuals by the use of experiments and surveys. A variety of research approaches that bridge information security and economics was also presented.

A review on the evolution of economic models of behaviour was presented and the main attributes and limitations of these models were analysed. Details on the notions of risk, ambiguity and uncertainty were provided. We focused on prospect and salience theory, as these theories are used throughout the study for examining experimental data.

Finally, we proposed a formalisation for modelling investment decisions in information security. Our approach focuses on two attributes of the information security environment, namely, security and operability.

Experiment 1: Decision-making under Risk and Ambiguity

Contents

3.1	Approach and Background	62
3.2	Methodology	63
3.2.1	Research Hypotheses	63
3.2.2	Experimental Procedure	64
3.2.3	Experiment Design	67
3.2.3.1	Hypothesis 1: Risk and ambiguity aversion	67
3.2.3.2	Hypothesis 2: Worst-case thinking and other heuristics	68
3.2.3.3	Hypothesis 3: Other-evaluation and behaviour	70
3.2.3.4	Hypothesis 4: Relative importance of security and operations	70
3.3	Analysis and Findings	74
3.3.1	Risk and Ambiguity Aversion	74
3.3.1.1	(A) Between-subjects tests	78
3.3.1.2	(B) Within-subjects tests	79
3.3.2	Worst-case Thinking	81
3.3.2.1	Lottery Comparisons and findings on potential heuristics	81
3.3.2.2	Consistency across types of decisions	84
3.3.2.3	Saliency Theory calculations for lottery-comparisons	85
3.3.3	Other-evaluation	88
3.3.4	Security - Operability Trade-off	89
3.3.5	Survey Analysis	93
3.4	Discussion	95
3.5	Summary	98

3.1 Approach and Background

This first experiment contributes in understanding the attitude of active information security professionals and practitioners across various levels of risk and uncertainty and in comparing risk behaviour of professionals against the behaviour of the general population.

A sample of students is randomly drawn from the database records of the Laboratory for Decision Making & Economic Research at Royal Holloway, University of London (RHUL), in order to be contrasted with a sample of security professionals. These are students that come from all departments and faculties of the university. We avoid using the terms “general population” and “student sample” as synonyms, based on the logic of [75].

The original paper describing this experiment was presented in the Workshop on the Economics of Information Security (WEIS 2015) [111] and a revised version was published in a special issue of the Journal of Cybersecurity [112].

The rest of this Chapter is organised in the following way. Section 3.1 describes the background and the approach taken in the experiment. Section 3.2 presents our core hypotheses and experiment design. The approach to data analysis is explained and the survey and experimental findings are presented in Section 3.3. Finally, a discussion on findings takes place in Section 3.4.

3.1 Approach and Background

A clear understanding of potential behavioural biases can constitute a useful tool for decision-makers as it can lead to the development of appropriate strategies for mitigating (or amplifying) the relevant biases.

For the purpose of eliciting risk attitudes of security professionals, potential vulnerabilities (probabilities) and losses (outcomes) are abstracted in the form of lotteries. The environment of information security has inherent characteristics which shape the context of decisions. We have designed our experimental scenarios focussing on several intrinsic attributes of the information security environment, which has operational losses and defence costs and direct losses, in the spirit of [13].

In particular, we focus on the following distinctive set of features, which are examined in our experimental approach:

1. *Loss domain*: each security investment decision can be described as a lottery with

3.2 Methodology

losses only. The best outcome is zero, thus, the scope of the decision-maker is *loss prevention*.

2. *Ambiguity of probabilities and outcomes*: security professionals face threats that are not precisely known. Often they do not know either the probability of a loss incurring or the likely size of the loss should it occur.
3. *Evaluation by other parties*: decision-makers in information security need to justify proposed security investment to others, e.g. to business managers or hierarchical superiors.

We find that professionals typically do a somewhat better job of maximising expected value than the student sample, although they too exhibit systematic behavioural biases and they have, to a certain degree, a distorted understanding of probabilities (Section 3.3).

At the end of the experiment we ask our subjects several survey questions relating to their professional role and to their willingness to trade off security and operability. There is considerable heterogeneity across professionals in their security / operability preferences associated with their professional roles. Most professionals are considerably biased towards one of the two domains and display loss aversion in their preferred attribute.

3.2 Methodology

3.2.1 Research Hypotheses

We analyse the behaviour of security professionals and students in our experiment and survey in order to test a series of hypotheses motivated by the following commonly observed behavioural patterns: ¹

1. *Risk and ambiguity aversion*: Risk aversion implies that given a lottery with a specific probability of loss, an individual is willing to pay more than the expected value of this loss to avoid playing the lottery. Ambiguity aversion implies that for a lottery with the same expected losses, an individual is willing to pay an additional amount above the risk premium to avoid the lottery (ambiguity premium) if, instead of a specified probability or outcome, there is a range of probabilities or

¹Loss aversion, i.e. a disproportionate weighting given to outcomes of less than zero, is another anomaly that has received considerable attention in the behavioural and experimental economics literatures. We do not focus on loss aversion in this research question because the information security environment involves losses only.

3.2 Methodology

outcomes. However, prospect theory implies that for large probabilities of losses, the same individuals may engage in risk-seeking behaviour [90]. It is possible that security professionals differ systematically from the student population with regards to risk and ambiguity aversion because the nature of their work implies greater exposure to risk and ambiguity. Security professionals face continual threats of losses, which are often not well defined.

2. *Worst-case aversion*: This implies that individuals pay disproportionate attention to the worst possible outcomes [32]. Their WTP to avoid playing a lottery increases in the maximum possible loss, even if the expected value and variance of a lottery is held constant. Worst-case thinking may be particularly common among security professionals [135], as the field has seen a number of high-profile cases of catastrophic losses due to security breaches in recent years. On the other hand, small losses due to security breaches may be regarded as a normal part of the operating environment and not be worthy of any expenditure.
3. *Other-evaluation*: This implies that when decisions are evaluated by other parties, individuals might tend to be more risk-averse, ambiguity-averse, and worst-case-averse. Since evaluators do not observe ex ante probabilities, only ex post outcomes, and thus may blame the decision-maker for bad outcomes even if the decision that led up to it was ex ante correct; “a decision maker, [...] makes the choice that is perceived to be most justifiable to others.” [50]. Other-evaluation may be particularly important in a security context, as security decision-makers normally have to justify their investment proposals to business managers, chief officers, the board of directors, etc.

We examine these behaviour patterns for both professionals and students in this experiment. In the case of security professionals, we also explore a fourth aspect of decision making in the survey part:

4. *Security and Operability*: We expect that security professionals will tend to value security more than operability. In other words, when balancing the costs of implementing security controls against the resulting loss of efficiency of business operation, security professionals will select a trade-off position that prioritises security ahead of operability.

3.2.2 Experimental Procedure

We conducted the experiment with two different samples. The sample of information security professionals was drawn from current and previous students of the distance

3.2 Methodology

learning MSc in Information Security at RHUL and consisted of 59 individuals (6 female) with an average age of 39. This group consists of security professionals who work in the industry and were undertaking the distance learning master’s program on a part-time basis or had finished the program in the past. The mean industry experience of this group is 9.6 years and professionals hold a variety of security positions in the industry (see Table 3.6). The student sample was drawn from individuals registered in the database of the Laboratory for Decision Making and Economic Research at RHUL. This group consists of 58 active full-time students (34 female) from all departments of the university with an average age of 22.4.²

Our experiment consists of several lotteries designed to test our hypotheses. The lotteries were framed neutrally for two reasons. First, we are trying to measure the underlying preferences of security professionals, not their interpretation of professional standards regarding threats. Secondly, the neutral framing means that student subjects are not being asked to make decisions on matters they have never previously experienced. Thus the student and professional samples can be considered directly comparable. All lotteries in the experiment require “one-off” decisions, with no feedback given after a choice is selected.

One set of lotteries elicits risk and ambiguity attitudes across three levels of expected losses and three levels of probabilities. Specifically, subjects are asked to choose between lotteries where ambiguity of both probability and loss are changed one at a time, or simultaneously. This approach enables us to compare WTP between-subjects and also within-subjects across different types of risky and ambiguous decisions.

In another set, the lotteries differ from each other in terms of worst-outcome, expected value and variance. These lotteries allow us to examine whether subjects employ simple decision rules (heuristics) to choose between the complex lotteries. Additionally, we elicit both WTP and binary choices for a subset of these lotteries, allowing us to check whether our subjects’ preferences are consistent across different framings.

A challenging point of the design was the creation of five-outcome lotteries for testing the worst-case thinking hypothesis. The variables that are changed across the lotteries are best-outcome, worst-outcome, expected value and variance. Moreover, certain lotteries were built on power-law distributions, as it has been shown that occurrences of many natural and social catastrophic phenomena follow such distributions [117]. Worst possible outcomes are deemed salient only if they are significantly different from the rest of the choice context, otherwise their associated events can be underweighted instead of overweighted by the participants. This means that both ranking and magnitude of losses are important. The degree of distortion of the perceived probabilities

²Three subjects in the student sample were excluded from the analysis because they stated that they were related to information security.

3.2 Methodology

was estimated by salience theory assumptions.

Participants were informed that they would receive a fixed participation payment of 3 USD and an additional potentially larger amount depending on their decisions in the experiment. In particular, one of the lottery comparisons of Appendix A.1.3 was randomly chosen for each participant, and their preferred lottery was “played” by a pseudo-random probability generator.³ The outcome was mapped to a maximum performance gain of 10 USD and was sent along with the participation payment to individuals, in the form of an Amazon gift certificate.

Furthermore, it is possible that security professionals have a tendency to overemphasise security issues at the expense of operational issues which could be important from a business perspective. To examine this question, we ask subjects to choose between security and operability in a realistic scenario. To make the distinction clear from potential operational risks [42], operability was framed as the *operational time* needed for task completion, and was measured explicitly in monetary terms, as was security. To exclude other factors, the scenario described an information system of moderate-impact to confidentiality, integrity and availability [129]. The experiment design measured not only the actual preference between security and operational time, but also the *relative loss aversion* in security and operability, by a series of questions dynamically linked to subjects’ previous replies.

Information security managers and decision-makers have to justify their investment proposals to business managers, chief officers, the board of directors or a similar body. The other-evaluation hypothesis as defined by Curley et al. [50] states that: “a decision maker, in making a choice, anticipates that others will evaluate his or her decision; and, so, makes the choice that is perceived to be most justifiable to others. This choice is for the option having the smallest degree of ambiguity”. The hypotheses aimed to reveal evaluation by others as a possible psychological source of behaviour that directly influences investment choices. Testing the other-evaluation hypothesis was ambitious in the context of an online experiment, because a way had to be found in order to provide an impression of an additional evaluation, on top of the standard statistical analysis that subjects were aware that they were being subjected to.

Finally, subjects filled out a short questionnaire about their personal attitudes and demographics. We use this data to examine correlations with behaviour in the main experiment.

³This mechanism was coded in Javascript on the Qualtrics platform which was used for the experiments and surveys. The code is available in Appendix A.1.7

3.2 Methodology

3.2.3 Experiment Design

We create a new instrument for measuring risk and ambiguity aversion, as a modification of the Holt and Laury instrument [78] and similar to the alternative of Moore and Eckel [115]. Some studies use outcome-ambiguous lotteries [56], while others use probability-ambiguous lotteries [10]. Our approach uses sets of lotteries with different levels of expected losses, in each of which there are four lotteries spanning from risky lotteries to lotteries ambiguous in probabilities, in outcomes and in both probabilities and outcomes. This design allows for between-subjects, as well as within-subjects analysis across lotteries of the same expected value. Experiment screenshots can be found in Appendix A.1.6. Data from professionals was collected online between 05/06/2014 and 27/06/2014. The student-sample data was collected on 26/08/2014. ⁴

3.2.3.1 Hypothesis 1: Risk and ambiguity aversion

We test risk and ambiguity preferences using 12 neutrally framed lotteries, divided into three groups of four. Lotteries within a group have identical expected value, but different degrees of ambiguity. Subjects are asked to state their maximum WTP in order to avoid playing each lottery. For example, the four lotteries in group A (H_{11} to H_{14}), which are presented to subjects as standalone lotteries, all have an expected value of $\mu = -2.5$ and contain the following text:

“What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is..:

- (i) *..a 5% probability of losing \$50 and losing nothing otherwise?”*
- (ii) *..a probability between 0% and 10% of losing \$50 and losing nothing otherwise?”*
- (iii) *..a 5% probability of losing between \$20 and \$80 and losing nothing otherwise?”*
- (iv) *..a probability between 0% and 10% of losing between \$20 and \$80 and losing nothing otherwise?”*

The lotteries in group B (H_{15} to H_{18}) and group C (H_{19} to H_{12}) contain the same potential outcomes, but probabilities of 15% (0%-30%) and 50% (35%-65%), respectively. Hence the ambiguous lotteries are all designed such that if there was a uniform distribution of outcomes and probabilities over the range of ambiguity, the expected

⁴A pilot experiment was distributed to PhD students and research associates at RHUL before launching the actual experiment. This provided us with useful feedback on the phrasing of tasks, participants' understanding, the average duration of the experiment and other presentation issues.

3.2 Methodology

value of losses would be the same as in the risky lottery. Table A.1 in Appendix A.1.2 contains the full set of groups of lotteries. In the following, we refer to lotteries of type (i). as *risky*, lotteries of type (ii). as *probability ambiguous*, lotteries of type (iii). as *outcome ambiguous*, and lotteries of type (iv). as *fully ambiguous*.

Subjects had to give their WTP for all 12 lotteries, but the order in which lotteries were presented was counterbalanced to control for potential order effects. That means that some subjects saw the risky lotteries first and some saw the fully ambiguous lotteries first.

3.2.3.2 Hypothesis 2: Worst-case thinking and other heuristics

This part of the experiment consists of five pairwise lottery comparisons (Appendix A.1.3) for which subjects were asked to choose their preferred lottery. All lotteries consisted of five outcomes; for conforming with salience theory [32], probabilities are kept the same in both lotteries, whereas outcomes are different, so that the expected value is the same in some pairs and different in others. For three of the lotteries involved in the comparisons there was a subsequent WTP question (Appendix A.1.4) similarly to the instrument of Hypothesis 1 (Appendix A.1.2). Thus, consistency of replies could be checked between comparisons and WTP per lottery.

For example, lottery L_6 (L_7) contains the following outcomes:

- 15% probability of losing nothing (nothing)
- 30% probability of losing 166.66 (183.33)
- 30% probability losing 300 (300)
- 20% probability of losing 450 (450)
- 5% probability of losing 900 (800)

While both lotteries L_6 and L_7 have the same expected value (-275), the highest loss in lottery L_6 (900) is greater than in lottery L_7 (800). In other words, lottery L_6 contains the “worse worst case”.

More abstractly, if μ_i is the expected value of lottery L_i , Var_i its variance, and ‘ \succeq ’, ‘ \succ ’ denote *weak* and *strict preference* respectively, then for example, for lotteries 9, 10 and 11 (Appendix A.1.3), theory predicts that:

$$L_{10} \succeq L_9, \text{ as } \mu_{10} = \mu_9 \text{ and } Var_{10} < Var_9$$
$$L_{10} \succ L_{11}, \text{ as } |\mu_{10}| < |\mu_{11}| \text{ and } Var_{10} < Var_{11}$$

3.2 Methodology

$L_9 \succ L_{11}$, as $|\mu_9| < |\mu_{11}|$ and $Var_9 \approx Var_{11}$

So, for an expected value maximiser, the worst lottery would be L_{11} , the least damaging would be L_{10} , and L_9 would lie in-between: $L_{10} \succeq L_9 \succ L_{11}$.

Instead of worst-case thinking, subjects may also use other heuristics or simple decision rules to decide between lotteries. For example, subjects may put a lot of weight on the best possible outcome (“best-case thinking”). Or they may pairwise-compare states across lotteries and prefer the lottery which “wins” in more states. Finally, subjects may also prefer lotteries with less variance, which would constitute a form of risk aversion. In order to test whether subjects use any of these heuristics, we compare the majority choice in our samples with the predictions of each heuristic. If any heuristic is consistent with all or at least most of the majority choices, it would provide evidence that subjects indeed rely on simple decision rules.

In total we have eight different lotteries which are used in five pairwise comparisons (two lotteries are used twice); three with an expected value of -275 and five with expected values ranging from -86.25 to -86.75 . Appendix A.1.3 contains further details.

In addition to the pairwise choices, we also elicit subjects’ WTP to avoid three of the eight lotteries (L_9 , L_{10} and L_{11} , see Appendix A.1.4). Since these three lotteries are also used in two pairwise choices, it allows us to check whether our subjects’ preferences are influenced by the type of decision. Such inconsistencies would violate rational choice theory since rational preferences should be unaffected by the way in which they are elicited (choice or WTP). The three WTP questions are separated from the pairwise choices by a different unrelated set of questions in order to disguise the similarities of the decisions, and both types of questions were counterbalanced.

Some lotteries in the experiment are designed to approximate power-law distributions. Such distributions simulate the occurrence of rare events that are observed in various physical and social phenomena, from earthquakes to citations and web hits [117]. Moreover, there is evidence for the existence of power-laws in cyber risks and in the growth of networks, relating these distributions with security issues like identity theft and malware spreading [107, 66]. Five out of the eight lotteries of Appendix A.1.3 are designed to approximate power-law distributions. In the general form of a power-law distribution, probability p is specified as a function of outcome x : $p(x) = \frac{\kappa}{(-x)^\alpha}$, where α is the distribution exponent and κ a constant. A rough requirement that is sustained by goodness-of-fit of various empirical data to such distributions [46] is that, $\alpha \in (0, 3)$. For the purposes of our experiment, and in order for the discrete distributions of monetary losses to approximate a power-law distribution, we have set $\alpha = 1.1$, constant $\kappa = 20$ and $x \in [-1000, 0)$.

3.2 Methodology

3.2.3.3 Hypothesis 3: Other-evaluation and behaviour

We examine other-evaluation using a between-subjects design in which subjects are assigned to either a *control group*, which is presented with the standard version of the experiment, and a *treatment group*, which is initially informed that all choices made in the experiment would be “further viewed” and would “go through an additional evaluation process“, according to the following statement:

“Important note: Your choices and their corresponding possible outcomes in the following experiment will be further viewed and will go through an additional evaluation process, after the completion of the experiment.”

Participants are informed that the evaluators would have the same information as themselves [45]. Ultimately any test of other-evaluation in an experiment such as this is going to be fairly weak for two reasons. First, the experiment itself has fairly low stakes, so any evaluation done within the experiment will not have much impact. This alone may not prevent other-evaluation from impacting subjects’ behaviour [17]. Additionally, however, since our experiment was conducted online, we could not give any public feedback, limiting the perceived social impact of the evaluation.

3.2.3.4 Hypothesis 4: Relative importance of security and operations

This part of the study consists of two sets of questions given to the professional sample only. The first part elicits preferences between enhancing security and enhancing operability of the system. It consists of scenario-based questions in which the participants have to choose between measures A and B, where A and B have different impact on the security level and the operability of the system. Both attributes have equal monetary values assigned to them. The specific questions asked are:

“Imagine the following scenario: You are managing an Information System that has moderate-impact on the confidentiality, availability and integrity of information records kept by your organisation.

The total worth of the system under protection is evaluated at \$10,000.

Full operability of the system allows the business to gain a profit of \$10,000.

Two new mechanisms A and B with the same cost are proposed for the system.

Which one of the following mechanisms do you prefer?” (Table 3.1)

Table 3.1: Initial question of Scenario 1: “Which one of the following measures do you prefer?”

Mechanism A	Mechanism B
Enhances Security of the system by 10%	Enhances Operability of the system by 10%

3.2 Methodology

Subsequent questions are formed dynamically depending on previous answers. In the next question the value of the preferred measure is marginally decreased, while the value of the other measure remains constant. This is repeated until the subject crosses over from choosing one measure to the other, so that a switching point between security and operability is specified.

The second set of questions elicits a measure for whether losses of the attribute preferred in Scenario 1 (security or operability) are treated differently to gains. Subjects are asked to choose between three options (Table 3.2).

Table 3.2: Scenario 2 template question

Choice A	Mechanism B	Choice C
Remains at the current system state	Reduces Security by $x\%$ Enhances Operability by $y\%$	Indifferent between A and B

Values x and y of choice B are taken from the switching point which is computed from Scenario 1. If a subject selects choice B or C, this stage of the experiment ends. If the subject chooses A, then the question is repeated, except if operability (security) has been preferred in the previous scenario, the security (operability) reduction is lowered by one percent. To illustrate, consider the following example: In Scenario 1 a subject is indifferent between a 5% security enhancement and a 10% operability enhancement. Subsequently, in Scenario 2, choice B gives a 5% reduction in security and a 10% enhancement in operability. If choice A is selected (i.e. choice B is considered worse than the status quo), the reduction in security in choice B is decreased to 4%, and so on.

The difference between the values of Scenario 1 and 2 (if any) constitutes our measure of loss aversion on the preferred attribute (security or operability). In particular, the difference i between value x of Scenario 1, and the final value $x - i$, $i = 0, 1, \dots$, as presented in Mechanism B in Scenario 2, is the magnitude of *loss aversion* on the preferred attribute (security or operability).

If losses and gains of equal magnitude are weighted equally, subjects will always select choice C. If, however, a loss looms larger than an equivalent gain, subjects will prefer choice A.

We assume that utility functions of security and operability are $Sec(\cdot)$ and $Ops(\cdot)$ respectively. The utility functions are defined on $[-1, 1] \rightarrow \mathbb{R}$, and also $Sec(a)$ and $Ops(a) > 0$ iff (if and only if) $a > 0$, $Sec(a)$ and $Ops(a) < 0$ iff $a < 0$ and $Sec(a)$ and $Ops(a) = 0$ if $a = 0$.

For example, assuming that the switching point elicited from Scenario 1 was $Sec(x)$

3.2 Methodology

and $Ops(10)$, $x \in [0, 9]$, then we can assume for simplicity ⁵ that:

$$Sec(+x\%) = Ops(+10\%). \quad (3.1)$$

Assuming that in Scenario 2, the current state A was preferred to Mechanism B:

$$Sec(-x\%) + Ops(+10\%) < Sec(0) + Ops(0) = 0 \quad (3.2)$$

$$\Rightarrow -Sec(-x\%) > Ops(+10\%) \quad (3.3)$$

$$\Rightarrow -Sec(-x\%) > Sec(+x\%). \quad (3.4)$$

Inequality (3.3) implies that the individual manifests *relative loss aversion* between the two attributes (security and operability), as $x \in [0, 9]$, and Inequality (3.4) that there is *loss aversion* on the utility of the preferred attribute (here on security). By the assumed utility functions we see that the absolute value of the utility of a reduction is greater than the utility of an enhancement of the same value. In other words, a reduction “hurts more” than an enhancement satisfies.

If Mechanism B had been chosen in the initial question of Scenario 2, this would mean that:

$$\begin{aligned} Sec(0\%) + Ops(0\%) &< Sec(-x\%) + Ops(10\%) \\ \Rightarrow Ops(10\%) &> -Sec(-x\%) \\ \Rightarrow -Sec(-x\%) &< Sec(x\%). \end{aligned} \quad (3.5)$$

Therefore, no relative loss aversion is manifested between the attributes or on the attribute of security. Quite the contrary: enhancement is preferred to reduction, so reduction “hurts less” than enhancement.

If Mechanism B was chosen in subsequent questions of Scenario 2, then e.g.:

$$\begin{aligned} Sec(0\%) + Ops(0\%) &< Sec(-(x-1)\%) + Ops(10\%) \\ \Rightarrow Ops(10\%) &> -Sec(-(x-1)\%), \end{aligned}$$

which also does not imply any loss aversion. However, if Mechanism A was again chosen in the first subsequent question of Scenario 2, then:

⁵It would be more precise, e.g. for $Sec(5\%) < Ops(10\%) < Sec(6\%)$, to have an approximation of $Ops(10\%) = Sec(\zeta\%)$, $\zeta \in (5, 6)$.

3.2 Methodology

$$\begin{aligned}
Sec(0\%) + Ops(0\%) &> Sec(-(x-1)\%) + Ops(10\%) \\
&\Rightarrow Ops(10\%) < -Sec(-(x-1)\%) \\
&\Rightarrow -Sec(-(x-1)\%) > Sec(x\%),
\end{aligned} \tag{3.6}$$

which would mean that the magnitude of loss aversion is increased in Inequality (3.6) in comparison to Inequality (3.5). This magnitude is captured in the variable named *LOSS_AV_SEC* for individuals that initially preferred security and similarly in variable *LOSS_AV_OPS* for operability (Figures 3.16, 3.17). So, an observed value of loss aversion κ , say in security, is translated as $-Sec(-\kappa\%) > Sec(+\lambda\%)$ or $|Sec(-\kappa\%)| > |Sec(+\lambda\%)|$, with $\kappa, \lambda > 0$ and $\kappa \in (0, \lambda]$.⁶

If Choice C was chosen in the initial question of Scenario 2, this would mean that:

$$\begin{aligned}
Sec(0\%) + Ops(0\%) &= Sec(-x\%) + Ops(10\%) \\
&\Rightarrow Ops(10\%) = -Sec(-x\%) \\
&\Rightarrow Sec(x\%) = -Sec(-x\%).
\end{aligned} \tag{3.7}$$

That is, preferences would be linear. Therefore, no further actions need to be taken in case of choices B or C.

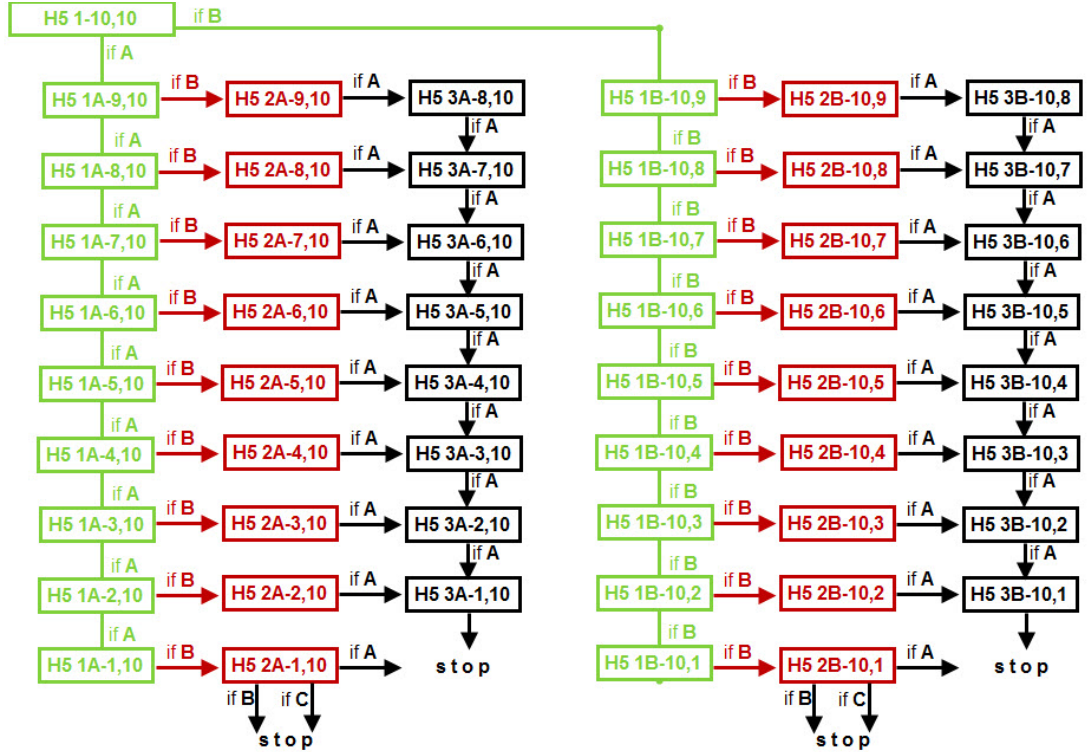
The ‘‘Display Logic’’ diagram that was used for the design of this experiment phase in the Qualtrics software [3] is presented in Figure 3.1.

Each box represents a question in the experiment. H5 is the coding used for this series of choices; ‘‘1A’’ denotes a preference for security in Scenario 1 and ‘‘1B’’ for operability. This first series of questions is used to trace the flip point where preference changes from security to operability or vice versa, and is stored as variable ‘‘H5 2’’. In the questions with coding ‘‘H5 2’’, the percentage value of the switching point is depicted (e.g. (9,10) indicates $Sec(9\%)$ and $Ops(10\%)$), and this pair is subsequently presented in a three-choice question of Scenario 2. Finally, the ‘‘H5 3’’ questions serve the purpose of gradual reduction of security or operability (coding 3A and 3B respectively) of Scenario 2, whenever choice A (‘‘Remains at the current system state’’) is selected. The process is terminated if choices B or C are selected at any point.

⁶The last pair of the utilities $Sec(\cdot)$ and $Ops(\cdot)$ that can possibly be compared by participants is $Sec(-1\%)$ against $Ops(+10\%)$ or vice versa. So, if the last choice is still the current state, the final (and maximum) loss aversion score is 9. With the current simplification in the formalism, this means $Sec(-\epsilon\%)$, with $\epsilon > 0$ and ϵ very small; ϵ cannot be interpreted as $\epsilon = 0$, as it was initially assumed that $Sec(0) = Ops(0) = 0$.

3.3 Analysis and Findings

Figure 3.1: Display Logic diagram for Hypothesis 4.



3.3 Analysis and Findings

This section presents our findings for the main hypotheses outlined in the previous section. Following standard experimental economics procedures, the experiment is counterbalanced to control for potential order effects (Appendix A.1.11: Order Effects), data has been checked for validity and cleaned accordingly (Appendix A.1.9: Data Cleaning), and outliers are shown to be non-influential (Appendix A.1.10: Outliers) for the relevant tests.

3.3.1 Risk and Ambiguity Aversion

The main hypothesis of risk and ambiguity aversion is examined both amongst independent subjects and per subject. The following lottery categorisation is used for both between- and within-subjects tests and its purpose is to examine whether the magnitude of losses and the nature of stakes (risky or ambiguous or both) have effects on the WTP of participants.

- *Group A*: lotteries H_{11} to H_{14} with expected value $\mu = -2.5$.

3.3 Analysis and Findings

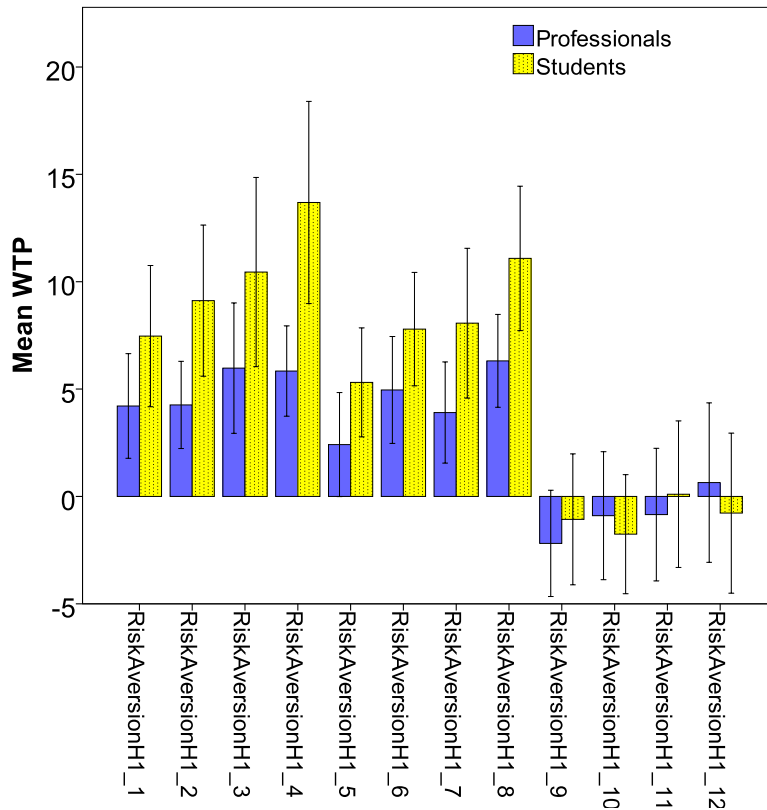
- *Group B*: lotteries H_{15} to H_{18} with expected value $\mu = -7.5$.
- *Group C*: lotteries H_{19} to H_{12} with expected value $\mu = -25$.

Group A corresponds to the first four lotteries of Table A.1 in Appendix A.1.2 (H1 Instrument), Group B consists of lotteries 5 to 8, and the last four lotteries of the table are in Group C. It should be noted that the first lottery of each group is a risky lottery, that is, it contains specific probability and outcome values. The second lottery of each group has specific losses and a probability interval, i.e. it is probability-ambiguous. The third lottery of each group is outcome-ambiguous, and the last lottery of each group is both probability- and outcome-ambiguous.

Findings on Risk Aversion

Finding 1: Both professionals and students are risk-averse for small- and moderate-probability losses and become risk-seeking for high-probability losses.

Figure 3.2: Mean risk-averse (positive) and risk-taking (negative) WTP of Students and Professionals per lottery. Bars represent participants' mean WTP minus the EV of each of the 12 lotteries.



Both information security professionals and students are willing to pay significantly more than the expected value of almost all first eight lotteries (Groups A and B) of

3.3 Analysis and Findings

Table A.1, which include both risky and ambiguous lotteries. In particular, significant risk aversion is manifested in the lotteries with small ($p = 0.05$) and medium ($p = 0.15$) actual or average probabilities, which correspond to small (\$2.5) and medium-range (\$7.5) expected losses. Table 3.3 in Section 3.3.1.1 depicts mean differences between stated WTP and expected value of each lottery for both samples. In other words, Table 3.3 reveals the lotteries for which WTP of subjects is significantly different from the expected loss.

However, both security professionals and students become risk-seeking when the probability of loss is large, switching from their risk-averse behaviour exhibited in the first eight lotteries (Figure 3.2). In the experiment, “large” probability is manifested as $p = 0.5$. The detailed methodology and the analysis of these results are presented in Section 3.3.1.1. This finding is in accordance with the universally observed phenomenon of the four-fold patten of risk attitude, as presented in Section 2.2.1.1.

Findings on Ambiguity Aversion

Finding 2: Professionals reveal ambiguity aversion in all of their choices; ambiguity aversion is not consistently observed in the student sample.

Finding 3: Professionals seem to deviate less from expected value maximisation (expected loss minimisation) than the student sample.

Security professionals become more risk-averse when they confront ambiguity, compared to when they confront risky lotteries. This result does not hold for the student sample in all cases.

We consider how WTP changes *within*-subjects, i.e. how each subject diversifies its WTP when presented with different types of risky and ambiguous lotteries. Figures 3.4, 3.5, 3.6, and 3.7 show differences between risky and ambiguous lotteries within subjects of both samples. In all three groups (A and B and C), professionals reveal significant differences in WTP between at least one pair of lotteries; differences are revealed, as expected, in the pair of each risky lottery with the lottery that is ambiguous in both probabilities and outcomes. Students reveal significant differences only amongst the lotteries of groups A and B. Detailed methodology and analysis for these results are presented in Section 3.3.1.2.

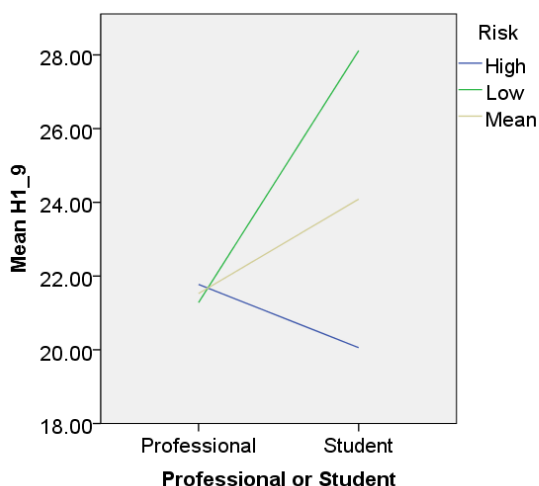
No clear conclusion can be derived regarding the behaviour towards the two types of ambiguous lotteries: the lotteries with ambiguous probabilities and the lotteries with ambiguous outcomes.

3.3 Analysis and Findings

However, professionals' WTP is closer to the expected value than the student sample. Specifically, professionals' WTP has smaller mean difference from the test value (zero), i.e. from the lottery's expected value, than the WTP of students in 13 out of the 15 lotteries (Table 3.3). Remarkably, the only two lotteries (H_{19} and H_{111}) in which professionals on average are willing to pay an amount that is more distant from the expected value, than the amount that students are willing to pay, are lotteries that are associated with a large probability of loss ($p = 0.5$). Starting with these lotteries, all consecutive lotteries reveal risk seeking behaviour. But, overall, professionals' estimations are closer to the expected value than students' WTP.

The result that security professionals remain closer to the expected value is also confirmed by the interactions between the variable "professional or student" and the variable of WTP with the self-reported risk attitude of the individuals. More precisely, moderation analysis reveals a significant interaction with predictor $X = Student$ or Pro , outcome variables $Y = WTP$, and moderator the Likert-scale self-reported risk attitude $M = General Risk$, interaction $b = 2.06$, 95% $CI [0.15, 3.97]$, $t = 2.14$, $p = 0.034$ (indicatively, interaction with variable $Y = H_{19}$ is shown in Figure 3.3).

Figure 3.3: Interaction of *Pro or Student* and H_{19} with *General Risk* as moderator



General Risk is the survey variable that corresponds to the question "How willing are you to take risks in general?" (low values indicate risk-averse and high values risk-seeking behaviour).

So, amongst risk seeking individuals, being an information security professional has a significant positive relationship with WTP to avoid a lottery; the effect is reversed amongst risk-averse individuals, i.e. amongst risk-averse individuals, being a professional has a significant negative relationship with WTP. In other words, amongst risk-seeking individuals, professionals are the least risk seeking, and amongst risk-averse individuals, professionals are the least risk-averse. This result constitutes an additional

3.3 Analysis and Findings

indication that, overall, professionals are closer to risk neutrality than the student sample.

3.3.1.1 (A) Between-subjects tests

There are overall fifteen WTP-type lotteries, all with negative-only outcomes. For each of these lotteries there is a corresponding variable Hx_y (for $x = 1, y = 1$ to 12, and for $x = 2, y = 6, 7$ or 8); and an additional variable called $RiskAversionHx_y$ is computed (as in Figure 3.2). The additional variable expresses the distance of the subject's WTP from the expected value (EV) of each lottery. Values are positive if the subject is willing to pay more than the actual expected value, and negative otherwise. So, positive values of this variable imply risk aversion and negative values reveal risk-seeking behaviour. A risk-neutral subject would have $RiskAversion = 0$.

Table 3.3: One-Sample t-test for between-subjects risk aversion

		One-Sample t-test (Test Value = 0)					
		Students N=58			Professionals N=59		
	EV	μ diff	95%CI of diff		μ diff	95%CI of diff	
			Lower	Upper		Lower	Upper
H_{11}	-2.5	7.4655***	4.1751	10.7558	4.2118***	1.7758	6.6479
H_{12}	-2.5	9.1206***	5.6006	12.6407	4.2627***	2.2323	6.2930
H_{13}	-2.5	10.4482***	6.0415	14.8550	5.9745***	2.9395	9.0095
H_{14}	-2.5	13.6896***	8.9826	18.3966	5.8389***	3.7376	7.9403
H_{15}	-7.5	5.3103***	2.7723	7.8483	2.4152	-0.0069	4.8374
H_{16}	-7.5	7.7931***	5.1508	10.4353	4.9576***	2.4686	7.4465
H_{17}	-7.5	8.0689***	4.5827	11.5551	3.9067**	1.5523	6.2612
H_{18}	-7.5	11.0862***	7.7232	14.4491	6.3135***	4.1512	8.4758
H_{19}	-25	-1.0689	-4.1174	1.9794	-2.1864	-4.6613	0.2884
H_{110}	-25	-1.7586	-4.5304	1.0132	-0.8983	-3.8769	2.0803
H_{111}	-25	0.1034	-3.3069	3.5138	-0.8474	-3.9392	2.2442
H_{112}	-25	-0.7758	-4.5041	2.9524	0.6440	-3.0682	4.3563
H_{26}	-86.6	40.3482	-4.4842	85.1807	16.3491	-10.4378	43.1361
H_{27}	-86.6	34.8827	-2.9151	72.6806	22.6372	-15.4711	60.7457
H_{28}	-89.75	24.0603	-8.9019	57.0226	18.7754	-12.2148	49.7656

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

Test is performed on H_{ij} variables' WTP differences from each lottery's expected value.

The statistical test used is the parametric one-sample t-test. This test determines whether a sample belongs to a population of a specific mean; the mean in our case is the expected value of the lotteries, but since $RiskAversionHx_y$ variables are computed from the expected values of each group of lotteries, the actual values of the new variables have zero as a reference point. As a result, all t-tests examine mean deviation from

3.3 Analysis and Findings

zero. The four assumptions for using the one-sample t-test require that the dependent variable is measured at interval or ratio level, data need to be independent, the number of significant outliers needs to be restricted and, lastly, the dependent variable needs to approximate the normal distribution. All assumptions are met since the dependent variable is WTP, measurement is between subjects and sample outliers are shown to approximate the normal distribution (see Appendix A.1.10).⁷

For *Group A* ($\mu = -2.5$) (Appendix A.1.2), the one-sample t-test reveals significant risk aversion for all lotteries for both professionals and students. The same result of significant risk aversion is observed for *Group B* ($\mu = -7.5$). However, in *Group C* ($\mu = -25$) statistical significance is not detected and behaviour shifts into being risk-seeking. We can see the positive differences of the mean in Table 3.3 (risk aversion) and how they become negative from the ninth lottery and on (risk-taking behaviour). The last three lotteries with large losses do not reveal significant risk attitudes (see the list of lotteries in Appendix A.1.2).

3.3.1.2 (B) Within-subjects tests

The within-subjects design increases the sensitivity of observed effects, as it is the same participants who provide the data for the various conditions. The tests used for these within-subject comparisons are the non-parametric Friedman test [63], which is used to measure differences between more than two conditions having a dependent variable of ordinal or continuous type, and the non-parametric Wilcoxon signed rank test [157], which also reveals the magnitude of pairwise WTP differences amongst lotteries. The tests require that the variables are related, i.e. that the same subjects provide the scores for the conditions. The Friedman test ranks all the conditions for each subject separately and then sums up the ranks for each condition. The independent variables are the expected values of all WTP lottery questions: H_11 to H_112 . The dependent variable is the amount that individuals are willing-to-pay in order to avoid each lottery. Lotteries are categorised, based on their expected values into the aforementioned groups.

For *Group A* both non-parametric tests reveal that students have significantly different (increased) WTP amongst the pairs of lotteries, but professionals are more “robust”, i.e. they only show significantly different behaviour between the risky and the fully-ambiguous pair (ambiguous in both probabilities and outcomes; Figure 3.5), whereas students also reveal significant differences amongst other pairs (Figure 3.4). The numerical values on the diagram nodes of all lottery pairwise comparisons indicate the

⁷The t-test is robust against violations of normality, nevertheless, we show that outliers are distributed roughly normally.

3.3 Analysis and Findings

sample average rank for each lottery of the group by the Friedman test, and pairwise significance is denoted by a yellow line.

Figure 3.4: Pairwise comparison of Group A lotteries for Students

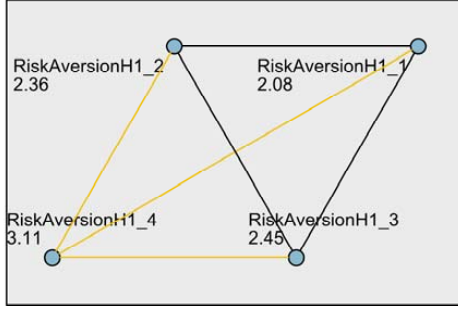
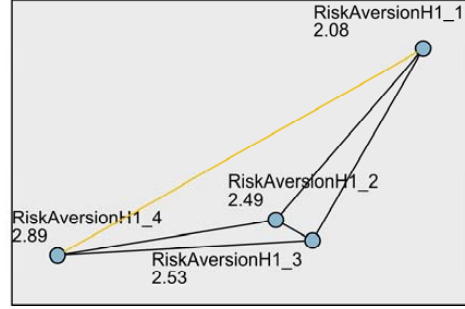


Figure 3.5: Pairwise comparison of Group A lotteries for Professionals



The aforementioned differences between students and professionals of *Group A* are almost reversed in *Group B*, where students reveal significant WTP differences in two out of the five possible pairs (Figures 3.6), and professionals in three out of five pairs (3.7). Moreover, these lotteries involve realistic moderate-range probabilities and professionals' choices are diversified for probability- and fully-ambiguous lotteries.

Figure 3.6: Pairwise comparison of Group B lotteries for Students

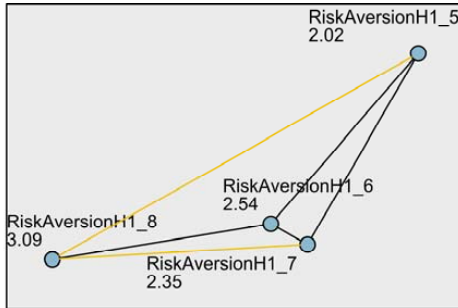
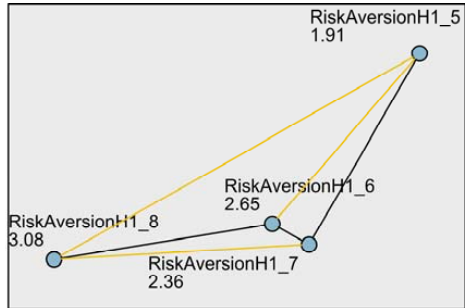


Figure 3.7: Pairwise comparison of Group B lotteries for Professionals

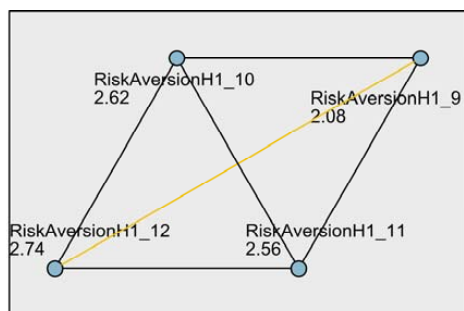


In *Group C* we observe that students do not diversify their WTP significantly due to ambiguity, but professionals significantly change their WTP between the risky and the fully-ambiguous lottery (Figure 3.8).

We observe that for both samples, as expected, WTP for avoiding a risky lottery is significantly smaller than for avoiding a lottery ambiguous in both probabilities and outcomes. It is not clear, however, whether ambiguity of probabilities increases WTP more than ambiguity of outcomes (we test a relevant hypothesis in “Experiment 2: Decision-making in Risk Treatment”, Chapter 4). Professionals are equally, or more, prone than students to increase their WTP in order to avoid mean preserving spreads of risky lotteries.

3.3 Analysis and Findings

Figure 3.8: Pairwise comparison of Group C lotteries for Professionals



3.3.2 Worst-case Thinking

This section is divided into the analysis of three parts: potential heuristics for lottery comparisons, preferences on lottery comparisons against stated WTP, and salience theory calculations for each lottery comparison.

3.3.2.1 Lottery Comparisons and findings on potential heuristics

Finding 4: Both professionals and students reveal choice preferences which are in line with expected values and state-by-state comparisons of lotteries.

Subjects are presented with five pairs of lotteries and are asked to choose the one they prefer (see Appendix A.1.3). The lotteries of each comparison pair have different attributes, e.g. they vary in their expected value, variance, best (least worst) and worst outcome. Depending on the lottery of each pair that is chosen by each sample, we examine whether this choice is in accordance, or in contradiction, with the relevant attribute. In Table 3.4 we can see preference percentages per comparison for both samples, as well as the “fit” of the various heuristics to the given preferences.

The major qualitative difference we observe between professionals and students is manifested in the first comparison (Lotteries 9 and 10, Appendix A.1.3). The third comparison is quantitatively different amongst the two samples. However, sample differences are not statistically significant (Pearson’s chi-2 test).

We can observe (Table 3.4) that in the comparisons in which expected value is different for each lottery, the lottery with the smallest expected loss is always chosen. Thus, the possibility that choice is based on the expected value is sustained. If lottery preferences are examined by the variance of the distribution of each lottery, we see that preferences

3.3 Analysis and Findings

are balanced. That is, choosing the lottery with the smallest variance is not clearly preferred as a heuristic.

Examining the *best possible outcome* of each comparison, i.e. the least damaging loss, we observe that in most of the cases, preferences of both professionals and students are almost in line with this heuristic. One might argue that these choices reinforce expected value as a heuristic, as three out of the five lotteries approximate power-law distributions, and therefore their smallest losses are associated with large probabilities ($p = 0.85$). However, such distributions underlie the lotteries of the first, second and fifth comparison which do not clearly comply with this simple heuristic.

In a similar fashion, the *worst-outcome* column examines whether subjects avoid the lottery with the worst outcome and choose the opposite lottery. It is notable that in all cases except one, the lottery with the largest loss is chosen by both professionals and students. This is arguably not surprising, as this heuristic is very simplistic.

Table 3.4: Lottery comparisons and accordance with heuristics

Lottery pair	Ex-pected Value	Vari-ance	Worst out-come	Best out-come	# of dom-inant states	Most salient pair (same dice roll)	Most salient pair (indep. dice rolls)
Students							
L_9 VS L_{10} (50%, 50%)	-	-	-	-	-	-	-
L_{10} VS L_{11} (60%, 40%)	✓	✓	×	×	✓	✓	×
L_8 VS L_6 (48%, 52%)	-	×	×	✓	-	×	×
L_6 VS L_7 (60%, 40%)	-	×	×	✓	-	×	×
L_4 VS L_{12} (52%, 48%)	✓	✓	×	✓	✓	✓	×
Professionals							
L_9 VS L_{10} (59%, 41%)	-	×	✓	✓	-	×	✓
L_{10} VS L_{11} (53%, 47%)	✓	✓	×	×	✓	✓	×
L_8 VS L_6 (36%, 64%)	-	×	×	✓	-	×	×
L_6 VS L_7 (61%, 39%)	-	×	×	✓	-	×	×
L_4 VS L_{12} (54%, 46%)	✓	✓	×	✓	✓	✓	×

‘✓’: preference justifies heuristic

‘-’: heuristic does not influence choice

‘×’: preference contradicts heuristic predictions

Pairs of percentages indicate preference for each lottery above

Most salient pair is a potential heuristic that is examined under the assumptions of salience theory. There are two separate columns for this choice rule. In the first

3.3 Analysis and Findings

column we assume “same dice roll” and salience is calculated by comparing all pairs of outcomes of *the same state* amongst the two lotteries and specifying the *most salient pair*. The most salient pair is the one which has a larger value of salience function $\sigma(x, y)$ for outcomes x and y (see Equations (2.6) or (3.8) in Sections 2.2.1.3 and 3.3.2.3, respectively). The most salient pair practically means that the difference of the involved outcomes is the most “noticeable” of all the differences, and consequently the subject chooses the lottery with the smallest loss. Note that same states correspond to the same probabilities in the compared lotteries. Same “dice roll” means that if, for example, the worst outcome materialises in the future for lottery A, then the worst outcome will also materialise for lottery B. So, in this heuristic the decision-maker compares the lotteries “line by line”. It can be argued that presentation of the comparisons (Appendix A.1.3) encourages the aforementioned rule of thumb for the decision-makers, as the states of the lotteries under comparison are presented one next to the other. However, results do not sustain such a decision rule, as preferences do not clearly favour the lottery with the smallest loss in the most salient pair. A closer look at the lottery distributions gives some indication that individuals might indeed be expected value maximisers. The third and fourth comparisons are never in accordance with the most-salient-pair rule, but the majority of comparisons: first, second and fifth, which follow power-law distributions, are. Since the first states are very probable, choices might imply that the decision-maker not only compares “line by line”, but also sums the outcomes when moving from one line to the next. For example, in the first comparison of Appendix A.1.3, the decision-maker, when reaching the second line, might add probabilities ($p_1 + p_2 = 0.93$) and since the combination of the first two states gives a very likely event, the decision-maker might choose the cumulatively smallest loss.

Similar reasoning holds for the *most salient pair* on “independent dice rolls”. This heuristic allows for the two lotteries to be executed independently, so that, for example, the best outcome might materialise in lottery A and the worst in lottery B. The difference here is that the most salient pair is calculated from all possible outcome-combinations amongst the two lotteries. The reasoning behind this particular heuristic is that, by fixing the least-worst outcomes to very similar values, it is the worst-case catastrophic outcome which potentially attracts the attention of the decision-maker. We can observe in Table 3.4 that the majority of results do not favour such a decision rule; there is only one indication that this heuristic complies with the choice of the majority of professionals.

Number of dominant states is the sum of the same-dice-roll states that are strictly preferable to the corresponding states of the opposite lottery. The “same dice roll” requirement is important here, as it is the corresponding states of “line-by-line” comparison that produce preference for one of the two lotteries. Note that not all lottery comparisons have a lottery that dominates the opposite lottery in the number of

3.3 Analysis and Findings

states, as in three of the comparisons lotteries have the same number of dominant states (having one or three identical states). Only the second and fifth comparisons have a states-dominant lottery. As we can see in Table 3.4 both these comparisons comply with this heuristic, for both samples. Thus, the lottery with the most dominant states is preferred by all participants.

3.3.2.2 Consistency across types of decisions

Finding 5: Security professionals exhibit preference inconsistencies between willingness to pay and choice decisions. The level of inconsistency is similar to the student sample.

There is an interesting finding pertaining lottery comparisons and WTP. For the three lotteries involved in the first two comparisons (Lotteries 9, 10 and 11, Appendix A.1.3) participants also state their willingness-to-pay to avoid them, at a different experiment stage (Appendix A.1.4). This allows for examining the consistency of these replies.

For the first comparison of L_9 against L_{10} , two variables are created, CONSISTENCY_ L_9 and CONSISTENCY_ L_{10} vs L_9 . In case a subject prefers L_9 to L_{10} in the comparison and is willing to pay less to avoid L_9 than to avoid L_{10} , the subject's replies are consistent and they are coded with a variable value of 0. In case of an inconsistency, the value is set to CONSISTENCY_ L_9 =1. Similarly, any contradiction regarding L_{10} is examined. So, inconsistency here is the phenomenon of preferring one lottery (from another) and at the same time be willing to spend more to avoid this lottery (than the other). The same reasoning is applied to the comparison and WTP between L_{10} and L_{11} . Note that L_{10} is used in both comparisons, and therefore there are two variables for L_{10} , one for each comparison. Table 3.5 depicts the percentage of subjects across both samples that choose L_i over L_j and reveal an inconsistency by their stated WTP.

Table 3.5: Lottery comparisons and willingness to pay inconsistencies.

Comparison variable	Comparison	Preference $L_i \succ L_j$	% of subjects that choose L_i over L_j and reveal choice inconsistency by WTP	
			Students	Professionals
H_21	L_9 VS L_{10}	$L_9 \succ L_{10}$	31%	46%
		$L_{10} \succ L_9$	55%	63%
H_22	L_{10} VS L_{11}	$L_{10} \succ L_{11}$	57%	36%
		$L_{11} \succ L_{10}$	17%	32%

There is no statistically significant difference amongst inconsistent percentages of professionals and students. However, the percentage of inconsistent professionals is larger than that of students in three out of four cases.

3.3 Analysis and Findings

3.3.2.3 Salience Theory calculations for lottery-comparisons

Finding 6: The majority of security professionals have a distorted perception of probabilities. The student sample reveals overall more consistent preferences than security professionals.

Salience theory is a theory of choice among lotteries that quantifies the decision weights of salient lottery outcomes, and proposes that the attention of the decision-maker is focused on the most salient outcomes. Such a focus favours the corresponding salient lottery for positive outcomes and disfavors it when lottery outcomes are in the domain of losses. For the purposes of the analysis of this section, it is assumed that the claims of salience theory [32] are true, and consequently conclusions on the subjects' *local thinking* are derived from the experiment results.

We briefly repeat the methodology for calculating salience theory-predicted preferences over two lotteries here; the full details are presented in Section 2.2.1.3:

- Step 1: write all possible state space pairs by combining all outcomes from the first and the second lottery.
- Step 2: rank all pairs by the salience function σ , with $\theta = 0.1$:

$$\sigma(x_s^i, x_s^{-i}) = \frac{|x_s^i, x_s^{-i}|}{|x_s^i| + |x_s^{-i}| + \theta}. \quad (3.8)$$

- Step 3: assign a number k to each pair, starting from the most salient pair. For example, the most salient pair across all states $\sigma(x_s^{max}, x_s^{min})$ has $k = 1$.
- Step 4: compute the sum:

$$\sum_{s \in S} \delta^{k_s} \pi_s [v(x_s^1) - v(x_s^2)], \quad (3.9)$$

where, π_s is the smallest probability of the two outcomes of the pair.

The following graphs are produced in Mathematica 9.0 [2] and depict the intervals of δ^8 for which the comparison L_i or L_j is expected to reveal preference: $L_i \succ L_j$. The x -axis represents values of δ and the y -axis represents the sum (3.9). Percentages of students and professionals that chose the first lottery and correspond to positive deltas are also given. The Mathematica code, the detailed calculations for the estimation of

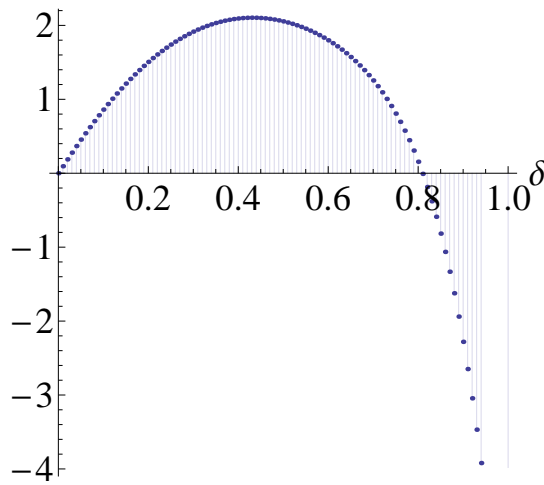
⁸As explained in Section 2.2.1.3, $\delta \in (0, 1]$ expresses the degree of probability distortion for a decision-maker, with $\delta = 1$ indicating objective probabilities.

3.3 Analysis and Findings

the δ intervals and the code for creating the corresponding graphs can be found in Appendix A.1.12. Note that here we assume “independent dice rolls”, i.e. pairs are formed by combining all outcomes of the first lottery with all outcomes of the second.

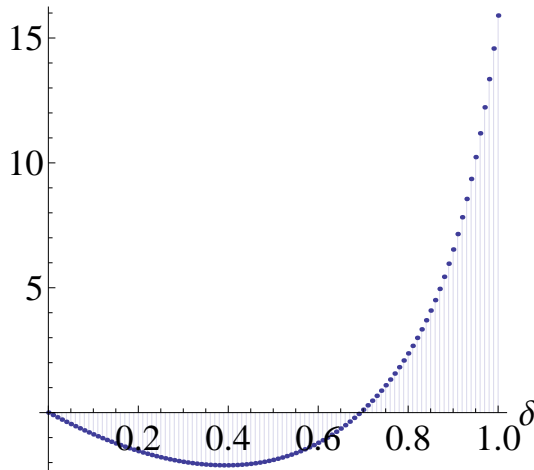
Figure 3.9 indicates that since the majority of professionals prefer L_9 , professionals are associated with $\delta \in (0, 0.8)$. This result suggests that preferences of professionals reveal a considerable degree of probability distortion. Students are equally split between the two lotteries, so their choice potentially corresponds to all possible delta values.

Figure 3.9: L_9 or L_{10} : values of sum 3.9 for $L_9 \succ L_{10}$, $\delta \in (0, 1]$
(Students: 50%, Professionals: 59%)



In Figure 3.10 we see that since the majority of both samples prefer L_{10} , and L_{10} is the first lottery in the comparison (i.e. corresponds to positive δ values), therefore, both professionals and students reveal a $\delta \in (0.7, 1]$, which is an interval that contains objective decision weights.

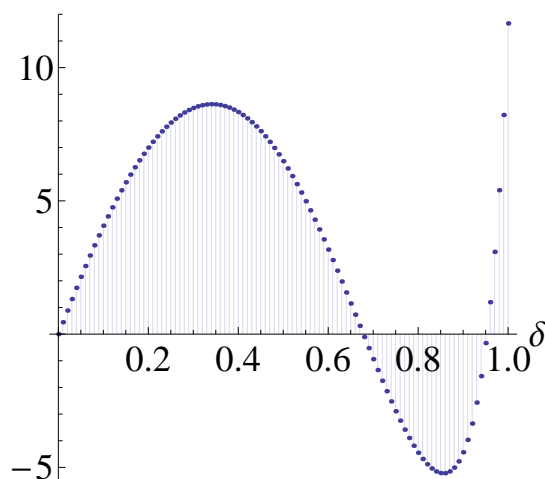
Figure 3.10: L_{10} or L_{11} : values of sum 3.9 for $L_{10} \succ L_{11}$, $\delta \in (0, 1]$
(Students: 60%, Professionals: 53%)



3.3 Analysis and Findings

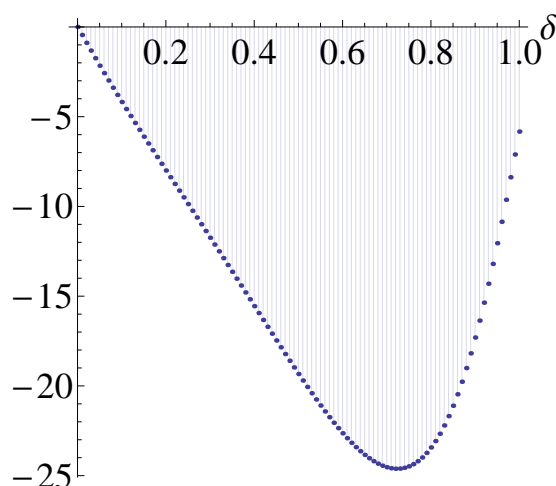
In Figure 3.11 the majority of both samples prefer the second lottery, therefore, choices correspond to deltas which give negative values, i.e. $\delta \in (0.66, 0.96)$. So, truly objective decision weights are excluded for both students and professionals; their preferences necessarily indicate some probability distortion.

Figure 3.11: L_8 or L_6 : values of sum 3.9 for $L_8 \succ L_6$, $\delta \in (0, 1]$
(Students: 48%, Professionals: 36%)



For the fourth comparison (Figure 3.12), the majority of both samples choose the first lottery, but no additional information is extracted, since the whole range of deltas corresponds to values which have the same sign.

Figure 3.12: L_6 or L_7 : values of sum 3.9 for $L_6 \succ L_7$, $\delta \in (0, 1]$
(Students: 60%, Professionals: 61%)

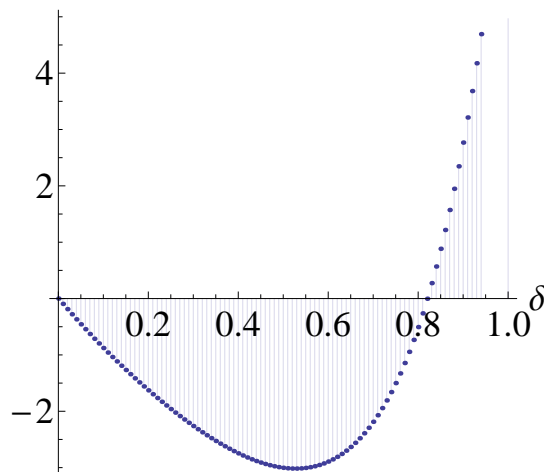


Finally, in Figure 3.13, the majority of both samples slightly prefer the first lottery, which would give $\delta \in (0.82, 1]$. Similarly to the second lottery comparison (with a more narrow δ interval) this result reveals decision weights even closer to objective

3.3 Analysis and Findings

probability perception.

Figure 3.13: L_4 or L_{12} : values of sum 3.9 for $L_4 \succ L_{12}$, $\delta \in (0, 1]$
(Students: 52%, Professionals: 54%)



Summarising the results, for information security professionals we observe that strong local thinking seems to be prevalent in the first comparison, i.e. $\delta < 0.8$. In the first and the third comparisons objective deltas are completely excluded. Only the second and fifth comparisons reveal local thinking which corresponds to delta-intervals that include the value $\delta = 1$, i.e. might imply objective perception of probabilities. However, distance from objective weighting is not negligible: the lowest potential value is approximately $\delta = 0.67$ and in the same comparison (L_8 or L_6) objective weighting of probabilities is excluded, allowing only for $\delta < 0.94$. For the student sample the intersection of the δ intervals is $(0.82, 0.96)$. This means that there is some local thinking, i.e. a distortion of objective probabilities that favours the lotteries containing smaller losses in salient pairs. Interestingly, and due to professionals' choice in the first lottery comparison, intersection of the δ -intervals for professionals is the empty set. We should note that interpreting this finding is not straightforward; it is, in any case interesting that preferences of the majority of professionals are not consistent enough to allow for a clear estimation of their degree of probability distortion.

3.3.3 Other-evaluation

Finding 7: There is no evidence that subjects change their risk behaviour when they are informed that they will be evaluated by other parties, in our online experimental setting.

No significant differences are observed between the control and the treatment groups

3.3 Analysis and Findings

of the hypothesis, in either lottery comparisons or WTP questions. The most probable explanation is that it is hard to create a sense of “evaluation by other parties” in an online environment. That is, participants already knew that their responses would be subjected to “evaluation” for either statistical analysis or validity checks.

Maybe a more effective experimental setting could be designed in a lab, where the experiment instructors could have served as an “observing party”. Or, presentation of the experiment lotteries in the treatment group could have included a “watching eye”, which would have given the participants of this group the impression that they are being observed, in the spirit of [58, 116].

3.3.4 Security - Operability Trade-off

Findings on preferences between Security and Operability

Finding 8: Security professionals reveal a preference for operability over security; this preference is significantly dependent on their job role.

Table 3.6: Security VS Operability preference across Security Job Titles

	Job Title					Total
	Senior executive role ^a	Managerial role ^b	IT & Security role ^c	Compliance, Risk or Privacy role ^d	Other	
Mechanism A Enhances Security of the system by 10% (chosen by 45%)	4	3	8	8	2	25
Mechanism B Enhances Operability of the system by 10% (chosen by 55%)	2	13	8	3	5	31
Total	6	16	16	11	7	56*

^a e.g. CEO, CIO, CISO, CSO etc.
^b e.g. Project Manager, IT Director, Security Manager etc.
^c e.g. Security Officer, System Administrator, Cyber Security Information Analyst etc.
^d e.g. Governance, Risk & Compliance Consultant, Information Security Consultant, Auditor etc.
* Three subjects did not answer this question.

Pearson $\chi^2(4, N = 56) = 9.946, p = .041$

In the choice between two mechanisms that either enhance the security of a system or its operational time (with the same monetary values assigned to each of the two attributes), professionals reveal a preference (55%) for operability over security enhancement. However, preferences could be influenced by the information security roles of the professionals, giving them a certain point of view. For this reason, we examine how this preference varies amongst the various job roles, and significant diversification

3.3 Analysis and Findings

between security and operability preference is found across the various positions. The role-related question presented to the participants is included in Appendix A.1.5 and preferences are shown in Table 3.6.

Results in Table 3.6 show that compliance and risk professionals are security-oriented, as might have been expected, due to the certification and regulatory issues they are exposed to. Also, not surprisingly, professionals with managerial roles prefer operability, as their positions are more project and task-oriented. However, IT professionals express a balanced preference between operability and security. Finally, senior executives choose security.

Findings on Security-Operability trade-off

Finding 9: Preferences for either security or operability are non-negligible.

Finding 10: Professionals tend to weight losses in their preferred attribute more strongly than gains.

This part of the analysis considers the estimation of a switching point between security and operability and the measurement of the magnitude of loss aversion in both security and operability.

Each participant reveals a “switching point” between security and operability. If the subject initially preferred security to operability, then their consecutive preferences are stored in the variable SWITCHPOINT_SEC.⁹ In Figure 3.14, values on the x -axis denote a switching point of enhancing security by $x\%$ ($x < 10$) and operability by 10%, after which operability enhancement becomes more attractive to the subject. So, x can be considered as a “balance point” for which the utility of $x\%$ of security equals the utility of 10% of operability: $Sec(x\%) = Ops(10\%)$.

Figure 3.15 depicts the operability equivalent. More precisely, both security-oriented professionals and professionals who choose operability reveal switching points close to the mean ($\mu = 4.5$), which suggests they both weight their favourite attribute “twice as much” as the attribute they do not choose (Figures 3.14 and 3.15). Practically, we could state that, on average, an enhancement of their favourite attribute by $x\%$ has the same utility as an enhancement of the not-preferred attribute by $2x\%$.

⁹Six participants in total did not take this task.

3.3 Analysis and Findings

Figure 3.14: Security switching points
($Sec(x\%), Ops(10\%)$)

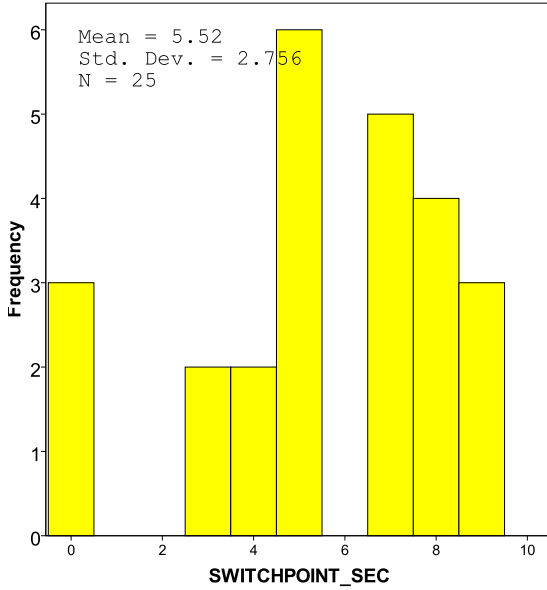
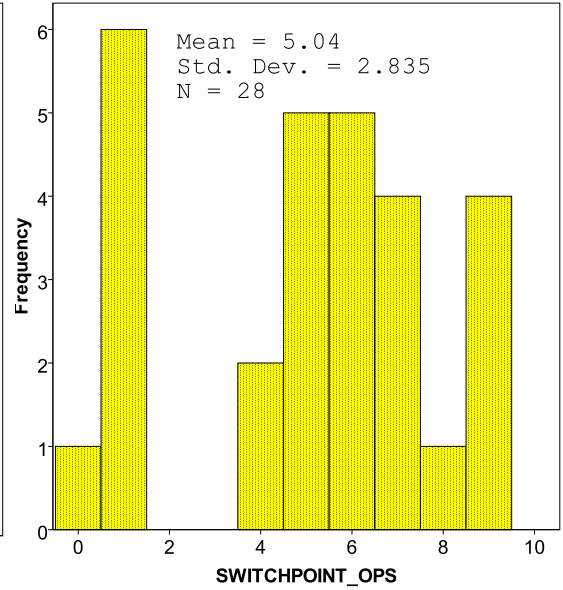


Figure 3.15: Operability switching points
($Sec(10\%), Ops(x\%)$)



The second measurement performed in this series of questions is the relative loss aversion between security and operability, as described in the design of Hypothesis 4 (Section 3.2.3.4). Variables LOSS_AV_SEC (Figure 3.16) and LOSS_AV_OPS (Figure 3.17) measure the difference between the aforementioned switching point and elicited preferences of Scenario 2 (see Table 3.2), which include reduction of the level of one of the attributes.¹⁰

Figure 3.16: Loss Aversion in Security
($Sec(-x + y\%), Ops(10\%)$)

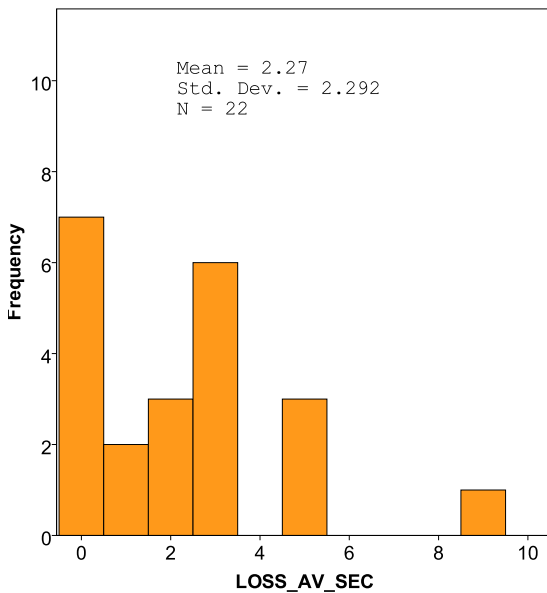
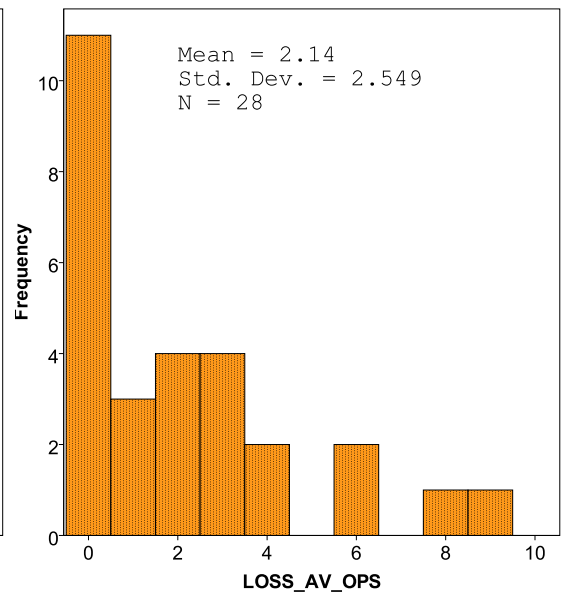


Figure 3.17: Loss Aversion in Operability
($Sec(10\%), Ops(-x + y\%)$)



¹⁰Another three participants did not finalise this task.

3.3 Analysis and Findings

The logic behind this measurement of relative loss aversion amongst the two attributes is the following: sometimes loss, or marginal reduction of an attribute level in our case, “hurts more” the individual than an equivalent enhancement “satisfies”.

Findings suggest subjects who reveal a preference for security exhibit *relative loss aversion* between the two attributes (security and operability) and *loss aversion* in the security attribute. More specifically, security-focused professionals weight reduction of security almost as much as they value triple the enhancement of operability; this is because the mean of loss aversion in security is $\mu_{LOSS_AV_SEC} = 2.27$ and the mean switching point for security is $\mu_{SWITCHPOINT_SEC} = 5.52$. Equation (3.6) implies that: $-Sec(-(x - i)\%) > Sec(x\%)$, where we can consider the mean value of x , instead of x , and the average magnitude of loss aversion as i .

And since, $-Sec(-(\mu_x - i)\%) > Sec(\mu_x\%) = Ops(10\%)$, thus:
 $-Sec(-(5.52 - 2.27)\%) = -Sec(-3.25\%) > Ops(10\%)$.

Which means that reduction of security “hurts” about three times more than enhancement of operability “satisfies” the decision-makers.

Loss aversion also holds for security itself: reduction of security is valued almost twice as security enhancement, and since, on average, $Sec(5.52\%) = Ops(10\%)$, thus, $-Sec(-3.25\%) > Sec(5.52\%)$. So, reduction of security, very roughly, “hurts” more than about double (a factor of 1.7) as its enhancement “satisfies”. This result is in accordance with prospect theory’s loss aversion findings on lotteries with gains and losses.

Using the above reasoning, professionals who choose operability reveal, on average, similar relative loss aversion between operability and security, as $\mu_{LOSS_AV_OPS} = 2.14$ and $\mu_{SWITCHPOINT_OPS} = 5.04$, thus:

$$-Ops(-(5.04 - 2.14)\%) = -Ops(-2.9\%) > Sec(10\%).$$

Their loss aversion in operability is, on average, about double (a factor of 1.74), as: $-Ops(-2.9\%) > Ops(5.04\%)$.

Finally, findings could indicate that professionals who have a preference for operability are likely to exhibit more linear preferences between reduction and enhancement of the attributes in their consecutive choices. The revealed mean of loss aversion in operability is smaller than that in security, many of operability-oriented professionals (11 out of 28) reveal zero loss aversion in operability and the distribution of loss aversion is concentrated around smaller values.

3.3 Analysis and Findings

3.3.5 Survey Analysis

A number of analyses are conducted on the survey data and its relations with the experiment results. Some of the findings are presented here.

Finding 11: Security professional reveal different risk attitudes to the ones they self-report.

Finding 12: Risk attitude for avoiding small and moderate probability lotteries is significantly diversified across educational levels of participants.

A significant correlation is found between *general risk attitude* and *WTP* for some of the twelve lotteries, for both samples. *General Risk* represents the survey question: “How willing are you to take risks in general?” (low values indicate risk-averse and high values risk-seeking behaviour). Student behaviour confirms literature findings on correlation of self-reported risk attitude and actual behaviour [52], but responses of professionals contradict the expected results. We observe in Table 3.7 that both students and professionals reveal some significant correlations between self-stated risk attitude and WTP. Students behave as expected, i.e. by revealing negative correlation (significant negative correlation in 3 out of the 12 lotteries), whereas professionals positive (significant positive correlation in 4 out of the 12 lotteries). This implies that, in some cases, professionals who report themselves as risk taking are actually willing to pay more in order to avoid the lotteries, so they behave in a risk-averse manner. It is noteworthy that this inconsistency is not observed in the student sample.

A number of linear regression models are conducted for the analysis of survey and experiment data, but results do not reveal significant predictors. The specifications for the models are described in Appendix A.1.14.

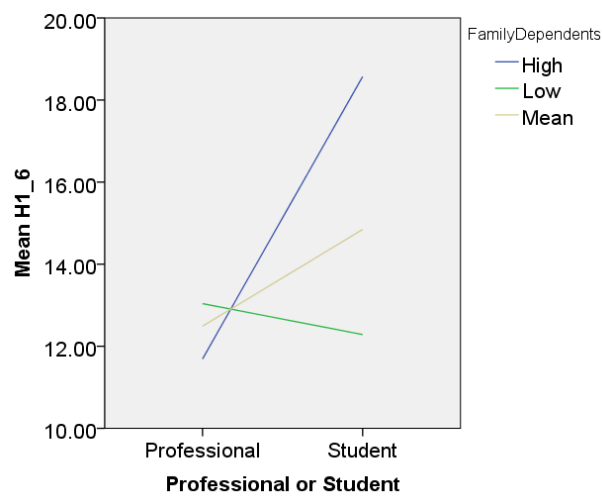
The demographic variable of the number of family dependents is found to cause an interaction. In particular, moderation analysis reveals a significant interaction between predictor $X = Student$ or $Professional$ and the outcome variables $Y = WTP$ (indicatively, variable H_{16}) and moderator $M = number\ of\ Family\ Dependents$, interaction $b = -3.22$, 95% $CI [-5.92, -0.5]$, $t = -2.37$, $p = 0.019$. In other words, when the number of family dependents is high, being an information security professional has a significant negative relationship with WTP; the effect is observed across all lottery level stakes, except for very high (indicatively, Figure 3.18). The expected result would be a positive relationship between number of family dependents and WTP, i.e. risk aversion, which is manifested for students, but surprisingly, does not hold for professionals.

3.3 Analysis and Findings

Table 3.7: Spearman's correlation coefficients for General Risk

	Students (N=58)	Professionals (N=59)
	Rho Sig. (2-tailed)	Rho Sig. (2-tailed)
H_{11}	-.030 .823	.117 .378
H_{12}	-.080 .550	.131 .324
H_{13}	-.086 .520	.227 .085
H_{14}	-.113 .400	.303* .020
H_{15}	-.080 .550	.213 .291
H_{16}	-.088 .512	.291 .025*
H_{17}	-.177 .183	.279* .032
H_{18}	-.114 .393	.363*** .004
H_{19}	-.266* .044	-.007 .616
H_{110}	-.252* .057	.131 .322
H_{111}	-.181 .174	-.005 .972
H_{112}	-.187* .160	-.008 .952

Figure 3.18: Interaction of *Pro or Student* and H_{16} with *number of family dependents* as moderator



3.4 Discussion

The educational level is also found to have a significant effect on WTP for small- and medium-probability lotteries. The non-parametric Kruskal-Wallis test on the merged sample of professionals and students reveals significant differences in WTP amongst the four levels of education: highschool, bachelor’s degree, master’s degree and PhD (Table 3.8). The overall trend is a higher WTP for participants with bachelors, and significant differences amongst the pairs of highschool-bachelor’s and highschool-PhD. An explanation could be that the observed result is caused by the student sample, the subjects of which are most likely at bachelor’s level. However, this explanation is rejected as there is no interaction between educational level and the attribute “professional or student” on WTP.

Table 3.8: Kruskal-Wallis Test with dependent variable WTP and 4 Educational levels

Kruskal-Wallis Test (N=117, df=3)	
Lottery	Test statistic
$H_1 1$	16.895***
$H_1 2$	6.070
$H_1 3$	7.887*
$H_1 4$	11.622**
$H_1 5$	8.062*
$H_1 6$	3.177
$H_1 7$	6.218
$H_1 8$	5.846
$H_1 9$	0.766
$H_1 10$	6.818
$H_1 11$	2.166
$H_1 12$	4.545

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

3.4 Discussion

The scope of this experiment was to specify behavioural aspects of decision-making under risk and ambiguity that information security professionals exhibit, and to contrast these attitudes against a student sample. In other words, the intention was to examine whether security professionals are rational decision-makers, and investigate whether certain underlying characteristics of information security shape a unique context. The experiment was divided into four major hypotheses, containing a number of sub-hypotheses and tests.

Security professionals exhibited significant risk aversion for small losses. This result, for the case of professionals, might mean that they consider small losses inevitable and therefore are willing to pay more to avoid them. This might have implications

3.4 Discussion

in a security environment, as such behaviour would always justify measures against low-impact threats. However, these losses are also associated with small probabilities, which could imply that professionals do not want to take risks, even if an event has very little likelihood of materialising.

The observed behavioural pattern of professionals complies with the four-fold pattern of risk attitudes for the domain of losses, introduced by Kahneman and Tversky [90]. Based on this pattern, professionals switched from being risk-averse and became risk-seeking for large probabilities. This finding implies that professionals “hope” to avoid a very likely loss, and they might consequently reject a favourable settlement. The settlement in this case could be a security investment amount that is equal to the expected loss, which the professionals might refuse to accept, as they would behave in a risk taking manner.

The combination of risk aversion for small-losses and the four-fold pattern could imply that preventive measures for common information security threats (e.g. malware, viruses) are viewed as necessary, unavoidable investment; but it would be quite alarming if professionals were to maintain their risk taking attitude for highly possible threat events. As was argued in Section 2.1.2.1, there is capacity for individual risk attitude to be manifested in the currently accepted risk assessment methodologies.

In relevant lotteries, professionals were always, whereas students were not always alarmed when they confronted ambiguous probabilities and outcomes. They expressed this fact by becoming significantly more risk-averse. However, it is reassuring that professionals consistently stated WTP closer to the expected losses than students did. Moreover, professionals did not seem to separate between ambiguity in probabilities and ambiguity in outcomes. These findings might indicate a “robustness” of professionals against ambiguity. The fact that professionals were alarmed by mean-preserving spreads, but they always remained closer to expected losses than students, might reflect their familiarity with similar presentation formatting of probabilities and losses.

Analysis on heuristics revealed that expected value and a line-by-line comparison of lotteries are consistent with professionals’ choices. All subjects chose the lottery with the number of most dominant states to its counterpart lottery; it is possible that these states provide focal points for the decision-makers. It cannot be inferred whether subjects used a more complex rule here, such as an estimation of “how strong” dominance was in each state. This finding is interesting, because if it holds in general it would imply that decisions could be “nudged” towards some direction. For example, an even amount of states might promote indecisions, as it would make it easier to have the same amount of dominant states. Another possibility would be to choose the states that represent the distribution of each lottery in such a fashion that favours the choice of one of the two lotteries.

3.4 Discussion

There were only indications that worst-case outcomes influenced the professionals' decisions, so, in this case, it seems that the rule that professionals followed approximates expected utility maximisation.

However, we would not characterise security professionals as rational decision-makers, with the strict definition of rationality. The inconsistencies they revealed between WTP and lottery comparison tasks were in some cases more contradictory than students' replies. The observed probability distortion, measured by the decision weights which are disproportionately assigned to salient outcomes, was even more puzzling, as the majority of professionals did not even manifest a consistent pattern in the way that students did. So, security professionals are very likely to have a biased perception of probabilities and, moreover, this perception is heavily influenced by the framing or presentation of the problem at hand. This fact implies that calculations involved in risk assessment methodologies are indeed susceptible to the subjective perception of the security decision-maker. Thus, this can be considered as another aspect of risk management that needs to be strengthened. A descriptive pluralism for relevant risk methodologies might be a starting point towards this direction.

Findings indicate that operability-focused individuals might reveal a more balanced understanding between security and operational time. This could suggest that a portion of the operations-oriented professionals are more objective in balancing losses and gains (reduction and enhancement) than their security-focused colleagues. In conjunction with the aforementioned finding on the influence of job position, this fact might imply a relation of operability with a "more practical" business-oriented approach which allows for a more objective (symmetric) contrasting of gains and losses.

Preference of the majority of professionals for operability might again be related to a business-oriented point of view, whereas the focus on security might indicate a more traditional approach.

Senior positions are usually associated with risk ownership and liability; also, positions higher in the hierarchy are able to see "the big picture" of the security environment. The fact that these individuals chose security over operability might indicate that professionals in such positions are inclined to consider the potential catastrophic and disastrous outcomes which can disrupt business functions, and therefore choose the "safer path" of security prioritisation.

3.5 Summary

In this chapter we presented an experiment and survey for examining risk behaviour of information security professionals and students.

We tested subjects' attitude towards risk and ambiguity. For that purpose we used unfavourable lotteries with various levels of probabilities and outcomes. Research hypotheses tested worst-case aversion and other-evaluation aversion. We examined possible heuristics that individuals use when they make risky choices. A mechanism was also devised for measuring preferences regarding the security-operability trade-off.

Both samples are found to have distinct risk behaviour and they cannot be considered as rational decision-makers. For both professionals and students, risk aversion is detected in small-probability and low-impact lotteries and risk seeking behaviour is observed for more probable and more damaging stakes.

One behavioural anomaly which we did not find evidence for in the experiments is that information security professionals were prone to worst-case thinking. When presented with lotteries with different worst-case scenarios, professionals consistently minimised expected losses. Neither do we find evidence that decisions in our lotteries are affected when subjects are told their choices would be further evaluated. However, the lack of influence of other-evaluation on decisions may be due to a weak treatment manipulation.

Preference inconsistencies between willingness to pay and choice decisions are evident for all participants. Professionals are better at estimating expected losses and they consistently react to ambiguity. Students, on the other hand, seem to have a less distorted perception of probabilities than professionals. Professionals insist strongly on their choice between security or operability. Operability is preferred over security, overall, and this preference depends on the job position of professionals.

In conclusion, both the information security context and individual risk attitude, seem to have a significant role in professionals' risk behaviour.

Experiment 2: Decision-making in Risk Treatment

Contents

4.1	Approach and Background	100
4.2	Methodology	102
4.2.1	Research Hypotheses	102
4.2.2	Experimental Procedure	103
4.2.3	Experiment Design	104
4.2.3.1	Hypothesis 1: Preferences over risk treatment . . .	104
4.2.3.2	Hypothesis 2: Preferences between probabilities and outcomes	105
4.2.3.3	Hypothesis 3: Framing of decisions as gains or losses	105
4.2.3.4	Hypothesis 4: Four-fold pattern of risk behaviour .	106
4.2.3.5	Order Effects	106
4.3	Analysis and Findings	106
4.3.1	Preferences over Risk Treatment Actions	107
4.3.2	Preferences between Probabilities and Outcomes	110
4.3.3	Framing of Decisions as Gains or Losses	112
4.3.3.1	More Analysis on the Three Framing Groups	115
4.3.4	Four-fold Pattern of Risk Attitude	121
4.4	Discussion	124
4.5	Summary	127

In the previous experiment (Chapter 3) decision-making biases and risk attitude of information security professionals are investigated in terms of WTP in order to avoid risky and ambiguous prospects. Professionals are found to be risk and ambiguity averse and they are also found to consider small losses as inevitable. The four-fold pattern of risk attitudes that was introduced by Kahneman and Tversky [90] is confirmed. Professionals are risk-averse for small and moderate probability lotteries ($p \leq 0.15$)

4.1 Approach and Background

and become risk-seeking when losses are associated with large probabilities ($p = 0.5$). Risk attitude of security professionals is also found to be measurably diversified from that of a student sample.

Decision-making in an information security context is often complicated, as it typically involves several separate decision points requiring individual attention. Risk management lies at the core of information security. Professionals need to assess risk and make decisions on how to *treat* risk, in order to minimise expected losses. Risk perception and judgement of individuals are inherently involved in this process. For these reasons, in this second experiment we examine whether professionals' risk attitudes hinder expected value optimisation of their decision-making. The contribution of this chapter is to estimate the extent of several potential biases which may impact the risk management process by measuring the extent to which risk attitudes deviate from expected value maximisation. We also show that professionals are likely to make different decisions over objectively similar risks depending on whether the decision is framed as a gain or a loss.

More precisely, preferences of information security professionals are solicited using risky lotteries. Framing of decisions as gains, losses, or individually separated losses is tested in order to examine whether it has an effect on professionals' WTP. Framing is found to diversify professionals' risk behaviour significantly. Experimental findings suggest that professionals reveal a preference for paying to reduce risk instead of paying to eliminate it. They also prefer to reduce the expected loss of threat scenarios rather than reducing the vulnerability associated with this loss. Overall, professionals are risk-averse when they face lotteries with small probabilities of loss and risk-seeking for lotteries with large probabilities.

This chapter is organised in the following way. Section 4.1 presents the background and theoretical framework of the study. Section 4.2 presents the methodology, hypotheses and design of the experiment and survey. Detailed data analysis along with findings are provided in Section 4.3. Finally, Section 4.4 presents a discussion of the main findings and their potential implications for organisations.

This experiment was presented in the Workshop on the Economics of Information Security (WEIS 2016) [113].

4.1 Approach and Background

In this experiment it is shown that throughout the risk management process there are certain decision points which are susceptible to individuals' subjective and potentially

4.1 Approach and Background

biased risk perception. Experimentally elicited risk attitude of information security professionals is examined and their behaviour is analysed against expected utility theory [155]. We target two activities in the risk management process: risk analysis and risk treatment.

An illustrative example-scenario, which expands the scenario presented in Section 1.1, and highlights the issues approached in this experiment is the following. An information security professional in an organisation needs to protect an asset of specific value against a threat. She possesses historical data on the frequency of this threat materialising, but data provides only an estimation of the threat probability. She has conducted an assessment on how vulnerable the asset is and she needs to decide whether additional protection is needed based on the expected value of loss. She might consider accepting the risk and not investing or she might propose investing in security measures for reducing the identified vulnerability. Alternatively, she can choose to implement measures for containing the potential damage in case it occurs, instead of making the asset less vulnerable. Finally, she can buy insurance in order to transfer the risk. In this scenario the professional might have preferences over the available actions, even if the expected value of the alternative choices is the same. The professional can view protection of the asset as a necessary cost subtracted from the budget, or she can view it as an investment with business return. Her view, might diversify her willingness to invest. In addition, the entire budget for protecting all assets might be initially allocated or a per-project budget could be allocated instead. The investment decision the professional makes is potentially influenced both by these factors and by her individual attitude towards risk. In such a case, decisions are very likely to be suboptimal by not maximising the organisation's profits.

The contribution of the experiment is the specification of the points which allow for the manifestation of potential biases throughout the risk management process (Sections 4.3.1 and 4.3.2) by measuring variations of risk attitude from the expected value of lotteries. Findings also show that framing of risk decisions as gains or losses can have a measurable effect on risk attitudes (Section 4.3.3). This is important for decision-making within firms, as distorted risk perceptions are very likely to become a direct or indirect influence on investment decisions.

4.2 Methodology

4.2.1 Research Hypotheses

We conduct an online experiment and survey in order to analyse the behaviour of security professionals with respect to the following hypotheses:

1. *Information security professionals reveal preferences over risk treatment actions:* In this hypothesis, the intention is to examine whether security professionals are favourably disposed towards accepting, eliminating or reducing risk. It is examined whether professionals prefer to eliminate risk completely (e.g. transfer risk by buying insurance) rather than reducing either the probability or the outcome of a lottery, if the expected value of the outcomes of the alternative actions is the same. Consequently, it is expected that participants are willing-to-pay relatively more for eliminating (avoiding) risk completely, instead of minimising it. We detected potential risk acceptance in professionals by examining whether their WTP is less than the expected loss of a lottery.

2. *Information security professionals reveal preferences between reduction of probabilities and reduction of outcomes:* Based on expected utility maximisation, a rational decision-maker should not differentiate between reducing the probability of a loss and reducing the loss itself in a case where both reductions reduce expected losses by the same amount. It is hypothesised that professionals will exhibit behavioural traits to favour the reduction of probabilities over the reduction of negative outcomes. The reason is that probabilities, but not consequences, dominate choices in “good or bad” lotteries. This can be explained by the existence of an experiential form of thinking involved in decisions (proportion dominance), as well as the analytical form of thinking [140].

Traditional information security approaches are mostly focused on prevention of losses (proactive security). A more recent approach also highlights the importance of loss containment (reactive security [23, 144]). Perception and consequently preference between reduction of probability and reduction of losses, is vital in information security, however it has not attracted proper attention. Such a potential preference is tested via WTP for reducing risk in abstract and scenario-type lotteries.

3. *Framing of decisions as gains or losses influences the risk attitude of professionals:* the effects that framing of lotteries as losses or gains has on risk attitude is tested. In other words, it is tested whether the manner of presentation or communication of a risk situation affects professionals’ choices.

A common view in information security is that investment in a security measure

4.2 Methodology

is perceived as a loss and that the maximum “gain” is a zero loss. However, information security can be also viewed as a gains-generating business component. The goal is to examine differences in the risk attitude of professionals, by randomly assigning them to groups of different framing and asking for their WTP to avoid or reduce risk in abstract lotteries. Three conditions for framing are used: losses, gains and a step-by-step losses procedure, which will be explained in detail in Section 3.2.3.3. Previous research on framing effects, starting from Kahneman and Tversky [150], concludes that decision-makers are generally risk averse in choices involving gains and risk seeking in choices involving losses.

4. *Four-fold pattern of risk behaviour*: The prediction of prospect theory states that decision-makers are risk-averse for small-probability losses and large-probability gains and risk-seeking for small-probability gains and large-probability losses [90]. Risk aversion for large-probability gains is caused by fear of disappointment, whereas risk aversion for small-probability losses is caused by fear of loss. In contrast, risk-seeking behaviour for large-probability losses and small-probability gains is caused by hope to avoid loss and hope to receive a gain, respectively. It is expected that this pattern is detected for the lotteries used throughout the experiment.

4.2.2 Experimental Procedure

The majority of the 78 participants (17 female) in the experiment and survey are working information security professionals who are current students and alumni of the on-campus and distance learning MSc programmes in Information Security offered by Royal Holloway, University of London (RHUL). The mean industry experience of these professionals is 7.6 years and their average age is 39.

We use abstract lotteries in order to examine context-free risk attitude of subjects, and scenario-type lotteries framed as information security problems to examine decisions in context. The lotteries used to elicit risk attitude are an adjusted version of those used in our previous experiment (Chapter 3). We set three levels of loss probabilities ($p_1 = 0.05$, $p_2 = 0.15$ and $p_3 = 0.5$) to reflect a realistic range of breach probabilities in information security¹. Participants are presented with 27 lotteries in three treatment groups (nine in each group), nine abstract lotteries that are common to all subjects and another nine common-for-all scenario-based lotteries; there is also one lottery used for participants’ payments. A complete list of the lotteries can be found in Appendix A.2.1.1.

Participants are informed that their reward is choice-dependent, but they do not know

¹The instrument follows the design logic of the Holt and Laury instrument [78] and shares similarities with the alternative instrument of Moore and Eckel [115].

4.2 Methodology

which lottery they will be paid for. Payment is based on their choice in one specific lottery in which they were asked to choose between three mean preserving spreads (see “Payment Lottery” in Appendix A.2.1.1). Participants’ choice indicates the range of potential outcomes and a pseudorandom javascript function determines the amount of payment (the code is available in Appendix A.2.4). Participants are asked about their preferred Amazon website at the end of the survey. All payments are sent to participants in the form of an Amazon gift certificate.

4.2.3 Experiment Design

Professionals’ replies were collected online between 22/01/2016 and 14/02/2016.² Screenshots from the experiment are included in Appendix A.2.2.

4.2.3.1 Hypothesis 1: Preferences over risk treatment

For the first hypothesis we use nine abstract lotteries labeled as L_{ij} and another nine scenario-based lotteries labeled SL_{ij} , with $i = 1, 2, 3$ and $j = A, B, C$ (see all lotteries in Appendix A.2.1.1 and definitions of variables in Appendix A.2.3). Each of the six lotteries L_1 to L_3 and SL_1 to SL_3 is presented to participants followed by three risk treatment actions: A, B and C. “A” refers to a lottery that proposes reduction of the *probability* of loss, and is phrased as: “*What is the maximum amount that you are willing to pay in order to reduce probability of loss from $p_1\%$ to $p_2\%$?*”.

In a similar fashion, “B” refers to the reduction of the *negative outcomes* of the lottery: “*What is the maximum amount that you are willing to pay in order to reduce potential loss from $\$x_1$ to $\$x_2$?*”.

“A” and “B” represent risk reduction (modification) actions. Lotteries with label “C” represent risk elimination (avoiding playing the lottery) and are phrased in the following way: “*What is the maximum amount that you are willing to pay in order to avoid playing the lottery completely?*”³.

In particular, for scenario lotteries SL_{ij} we consider an asset of specific value and we ask participants to state their WTP in order to modify or eliminate the risk from a potential breach of confidentiality, integrity or availability (Appendix A.2.1.1). We use asset value as the potential loss of the scenario, as it is common practice to assess risk

²As in Experiment 1, we distributed a pilot experiment before launching the actual experiment as a means of enhancing the presentation and increasing the understandability of the tasks.

³Reducing risk is related to the term “risk modification” and paying in order to eliminate risk (i.e. paying for not playing the lottery) is related to “risk transfer”, as will be also explained in the Discussion Section 4.4.

4.2 Methodology

considering the overall value of an asset [62, 148].

For the purposes of this study, we do not consider the risk treatment action of risk *avoidance* (as defined in ISO 27005 [81]), as it is usually related to changing business operations in order to keep away from certain threats. The risk treatment action of full risk *acceptance* is also available to participants, represented by a WTP of zero⁴.

4.2.3.2 Hypothesis 2: Preferences between probabilities and outcomes

The design of this hypothesis is embedded in the design of the first hypothesis. The scope here is to examine the pairs which only have to do with risk modification, i.e. with WTP for reducing probability of loss and WTP for reducing the magnitude of the negative outcomes. What is examined here is the differences amongst lottery pairs (L_{iA}, L_{iB}) , for the abstract lotteries, and (SL_{iA}, SL_{iB}) , for the information security scenario lotteries, for $i = 1, 2, 3$.

4.2.3.3 Hypothesis 3: Framing of decisions as gains or losses

This hypothesis is tested in the experiment by creating the following treatment: subjects are randomly divided into three groups. Each group is presented with nine lotteries, with a different framing. The first group of participants, *Group A*, is presented with the following setting:

“In the first stage of the experiment you are asked to make decisions in three lotteries. The lotteries have potential losses and you have an initial amount of money of \$30. In each lottery, you have to specify the maximum amount that you are willing to pay so that you can modify lottery values or avoid the lottery completely.”

This constitutes the loss-framing, as participants have to face either zero losses or suffer losses that are to be reduced from their given amount. In a similar fashion, *Group B*, the gain-framing group, presents participants with lotteries that involve gains-only, and participants start without any monetary amount (see Appendix A.2.1.1). Finally, the third group, *Group C*, is a mixture of gains and losses, in the following way: participants are given an amount of \$10 to play before they make choices in each of the three lotteries. The lotteries involve losses-only again, so this condition can be considered as a “step-by-step” loss-framing, in order to model decisions that are considered by decision-makers one at a time and independently from one another.

⁴No lottery from the three treatment groups, used for testing Hypothesis 3, was used in this hypothesis, although the lotteries of Hypotheses 1 and 3 have similar structure. This is because Hypothesis 3 lotteries were not fully randomised and participants often try to be consistent in their replies when they face similar questions.

4.3 Analysis and Findings

All group lotteries have a maximum gain or loss outcome of \$10 in order to diversify the outcome level from other hypotheses (which have a maximum loss of \$50). The nine lotteries of each group are presented in collections of three. The characteristic we measure across the three groups is the difference between WTP and the change in the expected value of each lottery from L_i to L_{ij} : $RA_{L_{ij}} = L_{ij} - EV_{L_{ij}}$ for $i = 1, 2, 3$ and $j = A, B, C$; equivalent variables are used for the scenario-type lotteries SL_{ij} (see Definitions in Appendix A.2.3). Positive values of the $RA_{L_{ij}}$ variables imply risk aversion, whereas negative values denote risk-seeking behaviour.

4.2.3.4 Hypothesis 4: Four-fold pattern of risk behaviour

The design of the previous hypothesis involves the creation and use of the aforementioned “risk aversion variables” (RA). These variables are analytically convenient as they have zero as a reference point, against which risk attitude is measured for the purpose of the fourth research hypothesis.

4.2.3.5 Order Effects

The whole design includes randomisation of certain parts in order to avoid order effects. Firstly, the three framing groups are randomly assigned to participants. A counter is used to check the number of replies in each group so that groups could be kept at similar sizes. The number of the received valid responses is $N = 78$, and these are split into $N_A = 25$, $N_B = 28$ and $N_C = 25$ for groups A, B and C, respectively. The lotteries of each group were subsequently presented in a fixed order.

The nine abstract lotteries and the nine scenario-type lotteries span across three levels of probabilities ($p_1 = 0.05$, $p_2 = 0.15$ and $p_3 = 0.5$), with three lotteries being assigned into each probability level (see Appendix A.2.1.1). Lotteries are presented in ascending probability level order. The presentation order of lotteries inside each level is fully randomised, i.e. for lotteries L_{ij} and SL_{ij} presentation order of L_iA , L_iB and L_iC is randomised for each $i = 1, 2, 3$ (see Appendix A.2.2.1).

4.3 Analysis and Findings

Analysis for each hypothesis is presented in this section. In all hypotheses except one, we use non-parametric tests since they do not require any assumptions about the

4.3 Analysis and Findings

sample distribution (e.g. normality)⁵. The experiment was created with the Qualtrics software v37 [3] and analysis was conducted with SPSS v21 [1].

4.3.1 Preferences over Risk Treatment Actions

Finding 13: Information security professionals reveal a preference for paying to reduce risk compared to paying to eliminate risk.

Finding 14: The possibility of eliminating risk by paying does not have an additional effect on professionals' risk attitude compared to the option of reducing risk.

Finding 15: Information security professionals are willing to accept some risk by being risk-seeking for large probabilities of loss.

The scope of the first hypothesis is to examine whether there is a preference amongst actions by which risk can be treated.⁶ In particular, participants are presented with losses-only lotteries and they are asked about their WTP regarding the risk treatment actions of risk reduction, elimination and acceptance. Risk reduction is expressed by two variables (lotteries) and risk elimination by another one, so we need to examine WTP differences per individual across these three variables (see Table 4.1). Risk acceptance corresponds to WTP that is less than the expected loss of a lottery.

The absolute difference between the expected value of the original lotteries L_i , $i = 1, 2, 3$ and the expected value of lotteries with modified risk (lotteries with index "A" and "B") is the same for each L_i , and we symbolise these differences as "*Delta_EV_*". The equivalent absolute difference for lotteries of type "C" is double that of "A" and "B" (Table 4.1). For this reason, for the analysis, we halve the WTP values that correspond to L_iC and SL_iC , $i = 1, 2, 3$ (variables indicated by "*_half*"; see definitions of variables in Appendix A.2.3). This way we compare WTP of each participant indirectly. We use the non-parametric within-subjects Friedman test [63], which is used to compare differences between more than two conditions for continuous or ordinal dependent variables. A risk neutral decision-maker with a linear utility function should reveal multiple WTP for dealing with multiple expected losses. In this case, risk elimination allows for avoiding the lottery completely, whereas risk modification (reduction) only halves

⁵The sample size $N = 78$ is sufficient for the parametric one-sample t-test at level $p = 0.05$ with statistical power 0.8, for the observed values of μ and σ [128].

⁶The numbering of findings is continued from the previous chapter in order to provide the reader with a broad view of the thesis findings. These findings are also summarised in the next chapter.

4.3 Analysis and Findings

Table 4.1: Initial and adjusted lotteries with probability p and loss x . ΔEV is the expected value difference between initial and adjusted lottery.

Experiment (Abstract) Lotteries L_{ij}			
Variable	Initial Lottery	Adjusted Lottery	$ \Delta EV $
L_1A	$p = 0.05, x = -50$	$p = 0.025, x = -50$	1.25
L_1B		$p = 0.05, x = -25$	1.25
L_1C		$p = 1, x = 0$	2.5
L_2A	$p = 0.15, x = -50$	$p = 0.075, x = -50$	3.75
L_2B		$p = 0.15, x = -25$	3.75
L_2C		$p = 1, x = 0$	7.5
L_3A	$p = 0.5, x = -50$	$p = 0.25, x = -50$	12.5
L_3B		$p = 0.5, x = -25$	12.5
L_3C		$p = 1, x = 0$	25

Survey (Scenario) Lotteries SL_{ij}			
Variable	Initial Lottery	Adjusted Lottery	$ \Delta EV $
SL_1A	$p = 0.05, x = -75,000$	$p = 0.025, x = -75,000$	1,875
SL_1B		$p = 0.05, x = -37,500$	1,875
SL_1C		$p = 1, x = 0$	3,750
SL_2A	$p = 0.15, x = -75,000$	$p = 0.075, x = -75,000$	5,625
SL_2B		$p = 0.15, x = -37,500$	5,625
SL_2C		$p = 1, x = 0$	11,250
SL_3A	$p = 0.5, x = -75,000$	$p = 0.25, x = -75,000$	18,750
SL_3B		$p = 0.5, x = -37,500$	18,750
SL_3C		$p = 1, x = 0$	37,500

the expected loss of the lotteries (see all lotteries in Appendix A.2.1.1); therefore objective decision-makers are expected to be willing-to-pay double in the risk elimination lotteries compared to their WTP in the risk reduction lotteries.

Figure 4.1: Ranks for L_1A, L_1B, L_1C_half

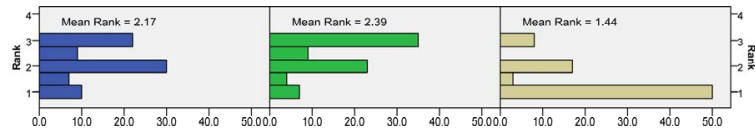


Figure 4.2: Ranks for L_2A, L_2B, L_2C_half

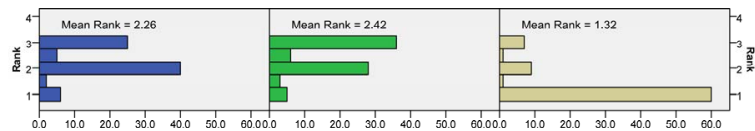
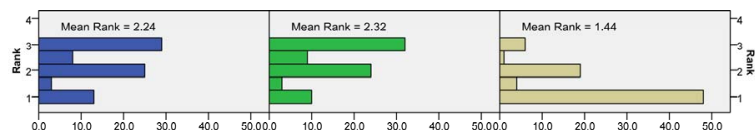


Figure 4.3: Ranks for L_3A, L_3B, L_3C_half



Results indicate that WTP for eliminating risk is significantly *smaller* than for reducing risk. This is clearly depicted in Figures 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6, as the smaller ranks

4.3 Analysis and Findings

Figure 4.4: Ranks for SL_1A , SL_1B , SL_1C_half

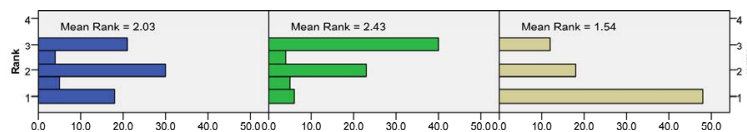


Figure 4.5: Ranks for SL_2A , SL_2B , SL_2C_half

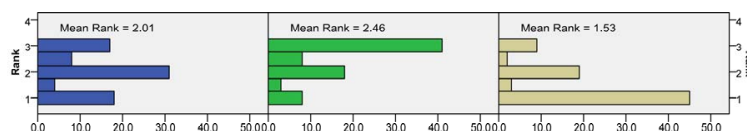
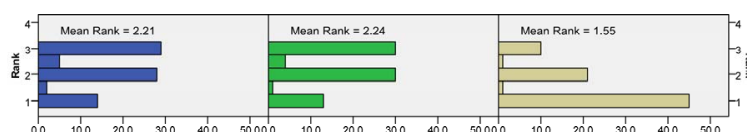


Figure 4.6: Ranks for SL_3A , SL_3B , SL_3C_half



of the “ C_half ” lotteries indicate smaller WTP. This difference is significant between all pairings of both probability and outcome reduction lotteries (“A” and “B” respectively) with the risk elimination lotteries “C”. The result is depicted in Table 4.2, which specifies the significant pairs, and the associated z-scores (standard deviations from the mean, in a normalised distribution) of the Wilcoxon signed rank test⁷. Mean values of each variable also allow for an interpretation of the direction of the differences. For example, given that variables “ C_half ” have smaller means than variables “A” and “B” for a given $i = 1, 2, 3$, this denotes that differences of the form $L_iA - LiC_half$ and $L_iB - LiC_half$ are always positive and so, subjects are willing to pay less for lotteries “ C_half ”. The same result holds for the scenario-type lotteries SL_{ij} .

The fact that halved WTP for eliminating risk is smaller than WTP for reducing risk implies an “indirect preference” for risk reduction. The interesting part is that in order to avoid double the expected loss, and because risk is eliminated completely in lotteries “C”, participants would be expected to state more than double the WTP than in “A” and “B”. That is, the certainty of risk elimination should have made participants more willing to pay to avoid the lotteries; but it did not. In other words, participants are not willing to increase their WTP in order to avoid lotteries completely, i.e. either risk elimination (lotteries “C”) does not have an additional effect on them, or risk elimination is perceived similarly to risk reduction (lotteries “A” and “B”) by the professionals. In this sense, we observe an insensitivity of decision-makers between risk reduction and elimination. The mean WTP for lotteries “C” not only is not double the mean WTP for lottery questions “A” and “B”, but it is of similar magnitude. Thus, professionals either underestimate the choice of completely eliminating risk or overestimate the act

⁷For samples with $N > 10$ we have acceptable approximations of the Normal distribution [59].

4.3 Analysis and Findings

Table 4.2: WTP mean values for all lotteries and Wilcoxon Signed Ranks Test for pairwise comparisons between the following within-subjects conditions: Probability Reduction (lotteries L_iA , SL_iA), Outcome Reduction (lotteries L_iB , SL_iB) and Risk Elimination by WTP (lotteries L_iC_half , SL_iC_half).

Experiment (abstract) lotteries			
Lottery variable	Mean	Compared Pairs	Z
L_1A	8.77	(L_1A, L_1B)	-1.221
L_1B	7.95	$(L_1A, L_1C_half)^{***}$	-4.771
L_1C_half	4.28	$(L_1B, L_1C_half)^{***}$	-4.916
L_2A	8.63	(L_2A, L_2B)	-1.503
L_2B	9.03	$(L_2A, L_2C_half)^{***}$	-5.985
L_2C_half	4.31	$(L_2B, L_1C_half)^{***}$	-6.392
L_3A	11.73	(L_3A, L_3B)	-.147
L_3B	11.55	$(L_1A, L_1C_half)^{***}$	-5.847
L_3C_half	6.53	$(L_1B, L_1C_half)^{***}$	-5.234

Survey (scenario) lotteries			
Lottery variable	Mean	Compared Pairs	Z
SL_1A	7764.99	$(SL_1A, SL_1B)^{**}$	-2.912
SL_1B	10533.88	$(SL_1A, SL_1C_half)^{***}$	-5.436
SL_1C_half	6070.60	$(SL_1B, SL_1C_half)^{***}$	-3.511
SL_2A	10753.14	$(SL_2A, SL_2B)^{***}$	-3.536
SL_2B	12783.05	$(SL_2A, SL_2C_half)^{***}$	-5.492
SL_2C_half	8065.85	$(SL_2B, SL_1C_half)^{***}$	-3.453
SL_3A	17240.65	(SL_3A, SL_3B)	-.715
SL_3B	19063.21	$(SL_3A, SL_3C_half)^{***}$	-4.859
SL_3C_half	12846.50	$(SL_3B, SL_3C_half)^{***}$	-4.520

Asymp. Sig. (2-tailed): * $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

of risk reduction.

At the same time, professionals remain risk-averse for small-probability lotteries and become risk-seeking for large probabilities of loss (Section 4.3.4). Therefore, overestimation of risk reduction or underestimation of risk elimination is prevalent across all probability levels and for both risk-averse and risk-seeking behaviour.

The risk treatment action of *risk acceptance* can be considered equivalent to a WTP that is less than the expected loss of a lottery. Such behaviour is observed in lotteries with large probability of loss, as is explained in Section 4.3.4.

4.3.2 Preferences between Probabilities and Outcomes

Finding 16: Information security professionals reveal a preference for reducing losses in threat scenarios, instead of reducing small or moderate probabilities associated with these losses.

4.3 Analysis and Findings

This second hypothesis is related to the previous one. In order to measure potential preferences between reduction of *probability* of loss and reduction of *loss* itself, we conduct a number of within-subjects tests in which it is the same subject who provides the input for each test condition. Namely, we compare WTP of each participant on the lottery pairs (L_{iA}, L_{iB}) and (SL_{iA}, SL_{iB}) , with the corresponding variables (A or B) serving as the independent variables of the tests. Lotteries with an “A” indicator refer to modification of probabilities and lotteries with a “B” refer to reduction of the potential negative outcomes. We use the non-parametric Wilcoxon signed rank test [156, 157] to measure pairwise differences amongst the two conditions of risk modification. The test calculates the absolute differences between related pairs and ranks them in increasing order; it then adds the ranks of negative and positive differences separately. Differences in professionals’ WTP amongst the two types of risk reduction are shown in Tables 4.3 (abstract lotteries) and 4.4 (scenario lotteries).

Table 4.3: Wilcoxon Signed-Rank Test for pairwise comparisons of abstract lotteries between the within-subjects conditions of probability reduction (L_iA) and outcome reduction (L_iB).

Wilcoxon Signed Ranks Test				
		N	Mean Rank	Sum of Ranks
$L_1B - L_1A$	Negative Ranks	23 ^a	33.72	775.50
	Positive Ranks	38 ^b	29.36	1115.50
	Ties	17 ^c		
	Total	78		
a: $L_1B < L_1A$, b: $L_1B > L_1A$, c: $L_1B = L_1A$				
$L_2B - L_2A$	Negative Ranks	28 ^d	32.09	898.50
	Positive Ranks	39 ^e	35.37	1379.50
	Ties	11 ^f		
	Total	78		
d: $L_2B < L_2A$, e: $L_2B > L_2A$, f: $L_2B = L_2A$				
$L_3B - L_3A$	Negative Ranks	32 ^g	36.33	1162.50
	Positive Ranks	35 ^h	31.87	1115.50
	Ties	11 ⁱ		
	Total	78		
g: $L_3B < L_3A$, h: $L_3B > L_3A$, i: $L_3B = L_3A$				

It is interesting that professionals reveal a statistically significant preference for the risk treatment action of reducing actual losses, instead of reducing the probability (vulnerability) that could lead to these losses. More importantly, this result is not revealed in professionals’ risk attitude on any of the abstract lotteries, but only when professionals face decisions framed as information security scenarios (this is also indicated, but not explicitly stated, in Table 4.2 of the previous hypothesis).

However, there is no significant difference revealed in the third pair of scenario lotteries. A potential explanation for this fact could be that lotteries SL_{3j} have a large probability of loss ($p = 0.5$), so perhaps professionals may estimate expected values more easily for these lotteries. Or it could be the case that professionals show such a preference only for small, and more realistic, in terms of actual threats, probabilities.

4.3 Analysis and Findings

Table 4.4: Wilcoxon Signed-Rank Test for pairwise comparisons of scenario lotteries between the within-subjects conditions of probability reduction (SL_iA) and outcome reduction (SL_iB).

Wilcoxon Signed Ranks Test				
		N	Mean Rank	Sum of Ranks
$SL_1B - SL_1A^{**}$	Negative Ranks	23 ^a	30.28	696.50
	Positive Ranks	45 ^b	36.66	1649.50
	Ties	10 ^c		
	Total	78		
a: $SL_1B < SL_1A$, b: $SL_1B > SL_1A$, c: $SL_1B = SL_1A$				
$SL_2B - SL_2A^{***}$	Negative Ranks	22 ^d	26.05	573.00
	Positive Ranks	45 ^e	37.89	1705.00
	Ties	11 ^f		
	Total	78		
d: $SL_2B < SL_2A$, e: $SL_2B > SL_2A$, f: $SL_2B = SL_2A$				
$SL_3B - SL_3A$	Negative Ranks	34 ^g	32.00	1088.00
	Positive Ranks	35 ^h	37.91	1327.00
	Ties	9 ⁱ		
	Total	78		

g: $SL_3B < SL_3A$, h: $SL_3B > SL_3A$, i: $SL_3B = SL_3A$

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

We thus see that there is no preference when abstract choices are concerned but, when it comes to information security scenarios, professionals reveal an inclination towards a reactive, i.e. “try to minimise losses if they occur”, rather than a proactive, “try to avoid losses”, approach to loss minimisation.

4.3.3 Framing of Decisions as Gains or Losses

Finding 17: Information security professionals are significantly more risk-averse when risky choices are framed as gains compared to when choices are framed as losses, in the process of either securing gains or eliminating losses.

Finding 18: Information security professionals are significantly more risk-averse when losses are subtracted from individual budgets compared to when losses are reduced from a single budget, in the process of eliminating losses.

The purpose of the corresponding hypothesis is to examine whether the samples of the three condition groups, i.e. framing of decisions as gains, losses, or individually separated losses are drawn from identical populations (see also Section 3.2.3.3). That is, whether there are differences with respect to the *mean* amongst the three treatment Groups, A, B and C. To test this hypothesis, we used the non-parametric between-subjects Kruskal-Wallis test for all lotteries in the groups (Table 4.5). In particular,

4.3 Analysis and Findings

we set a flag variable to denote which group the participant was assigned to, then we unified replies of the three groups into a single variable called $Groups_L_{ij}$, $i = 1, 2, 3$, $j = A, B, C$. Finally, we computed a new variable to express the difference of WTP from the expected value of each group lottery, symbolised by $RA_Groups_L_{ij}$. It is actually these “risk aversion variables” that are used in the non-parametric tests. These variables constitute a transformation of WTP around zero and allow for a comparison across groups, as group lotteries have the same absolute difference in expected value between their original version $Groups_L_i$ and their modified versions $Groups_L_{ij}$ (see all the lotteries in Appendix A.2.1.1).

Table 4.5: Kruskal-Wallis Test for comparing WTP mean differences across the three independent framing groups (see also Section 4.3.3.1).

Kruskal-Wallis Test (N=78, df=2)	
Lottery	Test statistic
$RA_Groups_L_{1A}$.314
$RA_Groups_L_{1B}$	2.413
$RA_Groups_L_{1C}$	23.015***
$RA_Groups_L_{2A}$.314
$RA_Groups_L_{2B}$	1.824
$RA_Groups_L_{2C}$	26.611***
$RA_Groups_L_{3A}$	5.873
$RA_Groups_L_{3B}$.466
$RA_Groups_L_{3C}$	25.616***

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

Analysis reveals that there is significantly different WTP manifested amongst all questions of type “C” across the groups (see Section 4.3.3.1).

For the lotteries that reveal significantly diversified WTP amongst the three groups, we can see the detailed differences in Figures 4.7, 4.8 and 4.9. Groups A, B and C, correspond to values 1, 2 and 3, respectively; numerical values on the triangle apexes indicate the sample average rank by the Wilcoxon signed rank test for matched-pairs, for lotteries L_iC across the groups. Significantly different pairs are connected with a yellow line.

It is apparent from the average ranks in Figures 4.7, 4.8 and 4.9 that WTP of professionals is significantly larger in the second group, i.e. in the group of the gain-framing. Probabilities of winning in this group are all large ($p_1 = 0.95$, $p_2 = 0.85$ and $p_3 = 0.5$), so it was expected that participants would become very risk-averse because of fear of disappointment of not winning anything. In the other groups where we have loss-framing, WTP is significantly smaller. In other words, increased risk aversion in the gain-framing group (denoted by “2” in the triangles), compared to the loss-framing group (denoted by “1”) was expected. However, the interesting finding is that risk attitude is also significantly diversified between the loss-framing group (“1”) and the

4.3 Analysis and Findings

step-by-step-loss-framing group (“3”). Distribution of WTP across the three groups is depicted in Figures 4.10, 4.11 and 4.12.

Figure 4.7: Wilcoxon Signed Rank Test pairwise risk aversion comparisons for L_1C (risk elimination) across the three groups.

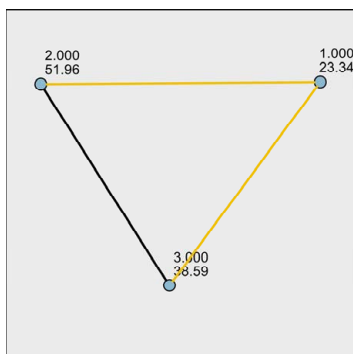


Figure 4.8: Wilcoxon Signed Rank Test pairwise risk aversion comparisons for L_2C (risk elimination) across the three groups.

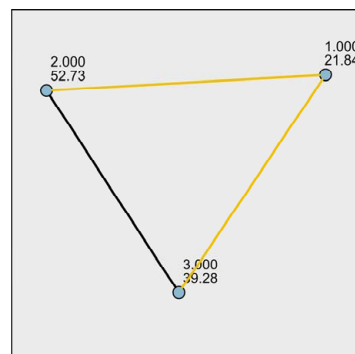


Figure 4.9: Wilcoxon Signed Rank Test pairwise risk aversion comparisons for L_3C (risk elimination) across the three groups.

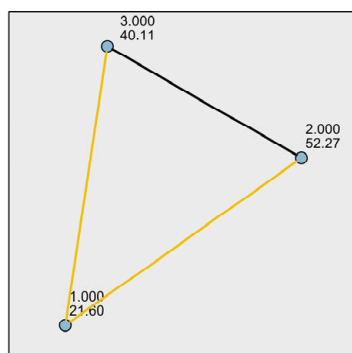
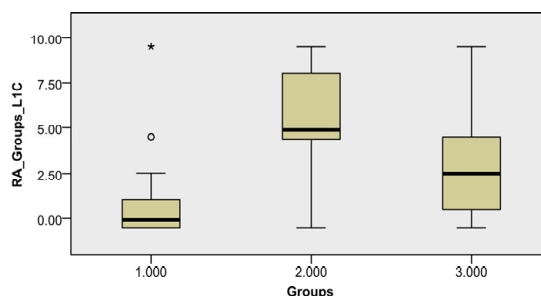


Figure 4.10: Risk Aversion Boxplots for Lottery $Groups_{L_1C}$ across the three independent groups. Wilcoxon Signed-Rank Test significant values for comparisons of pairs: Groups A-C ($Z = -2.53$, $p = 0.034$), Groups A-B ($Z = -4.797$, $p < 0.01$).



Although the lotteries involved in the three treatment groups were not randomised in order, the risk attitude pattern manifested in all other lotteries also holds for the group lotteries. Manifested behaviour confirms the four-fold pattern of risk behaviour that is presented in detail in Section 4.3.4 (Table 4.6).

4.3 Analysis and Findings

Figure 4.11: Risk Aversion Boxplots for Lottery *Groups_L2C* across the three independent groups. Wilcoxon Signed-Rank Test significant values for comparisons of pairs: Groups A-C ($Z = -2.706$, $p = 0.02$), Groups A-B ($Z = -5.158$, $p < 0.01$).

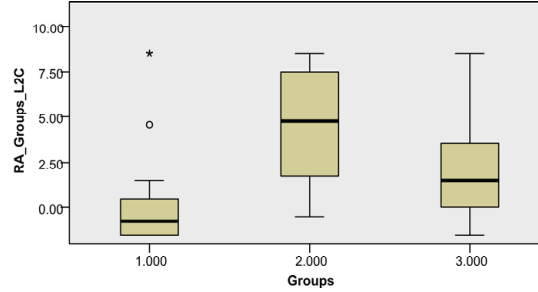
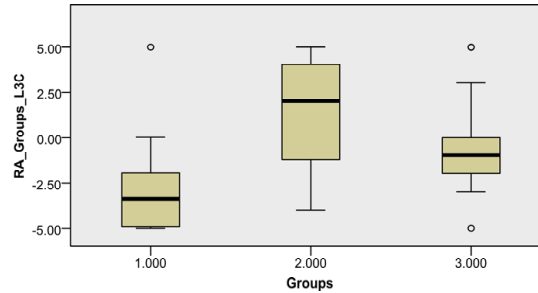


Figure 4.12: Risk Aversion Boxplots for Lottery *Groups_L3C* across the three independent groups. Wilcoxon Signed-Rank Test significant values for comparisons of pairs: Groups A-C ($Z = -2.665$, $p = 0.08$), Groups A-B ($Z = -5.061$, $p < 0.01$).



4.3.3.1 More Analysis on the Three Framing Groups

In order to examine these differences in more detail amongst pairs of groups, we created another three variables in the following way. In case Group A was presented to the participants, we set variables AB and AC equal to 1. If Group B was answered then AB and BC are set to 2, and if Group C was activated, variables AC and BC are set to 3. This way each participant has two of these Groups set to 1, 2 or 3 and, for example, by using Group AC we can compare between subjects, considering only subjects assigned to Group A or Group C. Mann-Whitney tests reveal a distribution-wise comparison between the three pairs of groups in Figures 4.14, 4.15, 4.16, 4.17, 4.18, 4.19, 4.20, 4.21 and 4.22. The Kruskal-Wallis test for all three Groups is presented in Figure 4.13.

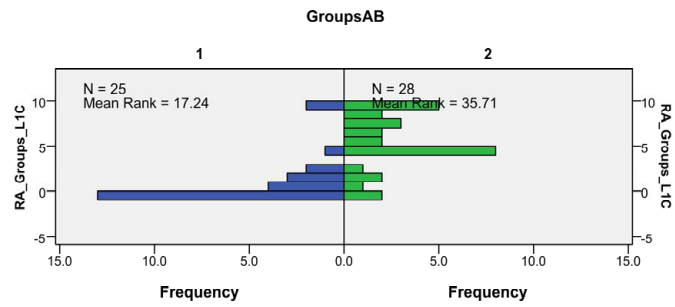
4.3 Analysis and Findings

Figure 4.13: Kruskal-Wallis Test for Risk Aversion between the three Groups.

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of RA_Groups_L1A is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.855	Retain the null hypothesis.
2	The distribution of RA_Groups_L1B is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.299	Retain the null hypothesis.
3	The distribution of RA_Groups_L1C is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.
4	The distribution of RA_Groups_L2A is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.855	Retain the null hypothesis.
5	The distribution of RA_Groups_L2B is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.400	Retain the null hypothesis.
6	The distribution of RA_Groups_L2C is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.
7	The distribution of RA_Groups_L3A is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.053	Retain the null hypothesis.
8	The distribution of RA_Groups_L3B is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.792	Retain the null hypothesis.
9	The distribution of RA_Groups_L3C is the same across categories of Groups.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.

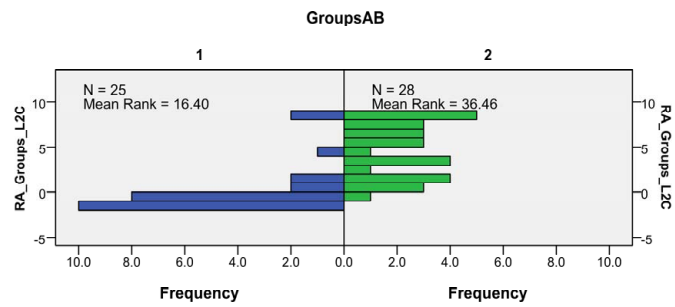
4.3 Analysis and Findings

Figure 4.14: Mann-Whitney Test for Risk Aversion between Groups.



Total N	53
Mann-Whitney U	594.000
Wilcoxon W	1,000.000
Test Statistic	594.000
Standard Error	55.825
Standardized Test Statistic	4.371
Asymptotic Sig. (2-sided test)	.000

Figure 4.15: Mann-Whitney Test for Risk Aversion between Groups.



Total N	53
Mann-Whitney U	615.000
Wilcoxon W	1,021.000
Test Statistic	615.000
Standard Error	56.004
Standardized Test Statistic	4.732
Asymptotic Sig. (2-sided test)	.000

4.3 Analysis and Findings

Figure 4.16: Mann-Whitney Test for Risk Aversion between Groups.

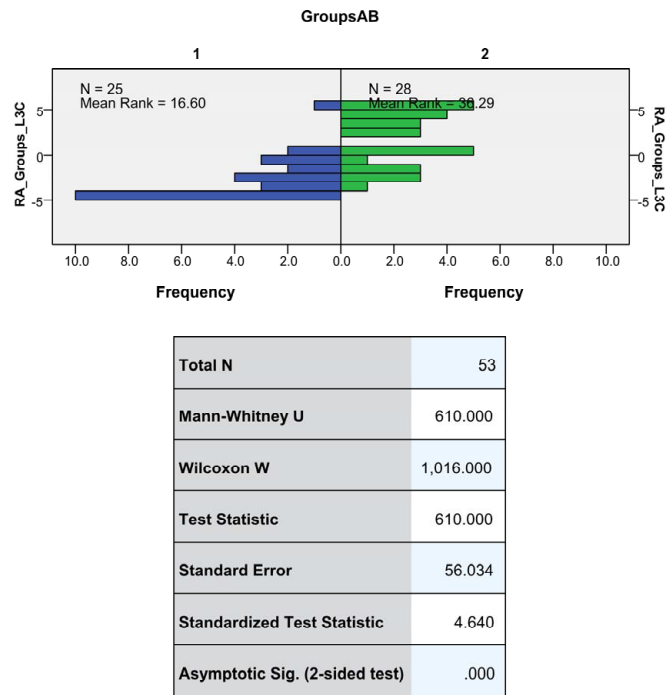
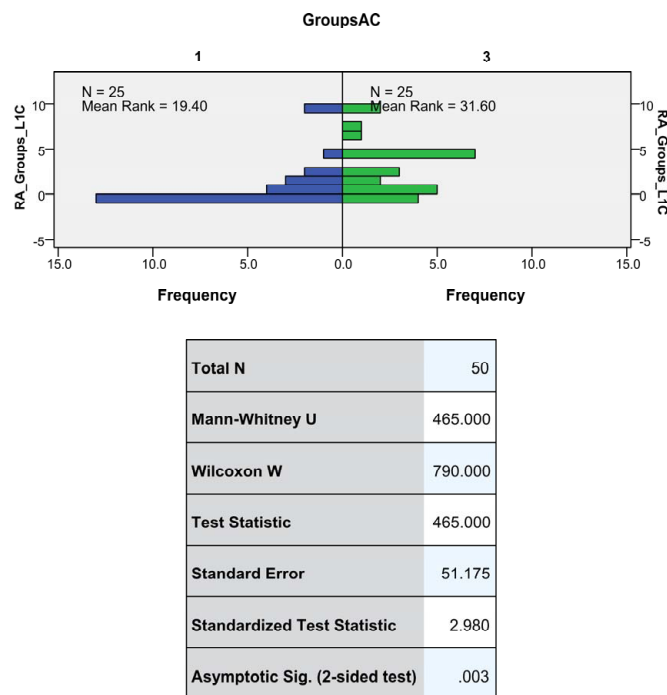
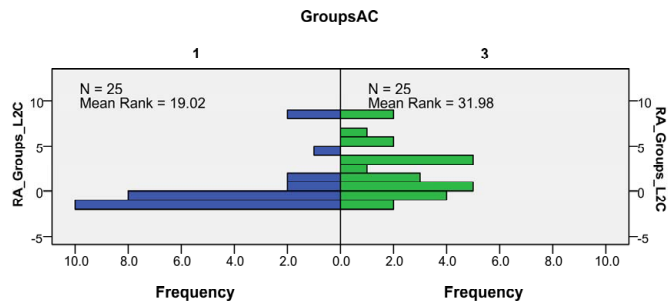


Figure 4.17: Mann-Whitney Test for Risk Aversion between Groups.



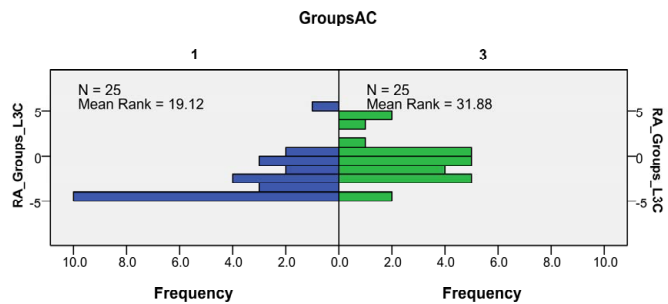
4.3 Analysis and Findings

Figure 4.18: Mann-Whitney Test for Risk Aversion between Groups.



Total N	50
Mann-Whitney U	474.500
Wilcoxon W	799.500
Test Statistic	474.500
Standard Error	51.403
Standardized Test Statistic	3.152
Asymptotic Sig. (2-sided test)	.002

Figure 4.19: Mann-Whitney Test for Risk Aversion between Groups.



Total N	50
Mann-Whitney U	472.000
Wilcoxon W	797.000
Test Statistic	472.000
Standard Error	51.441
Standardized Test Statistic	3.101
Asymptotic Sig. (2-sided test)	.002

4.3 Analysis and Findings

Figure 4.20: Mann-Whitney Test for Risk Aversion between Groups.

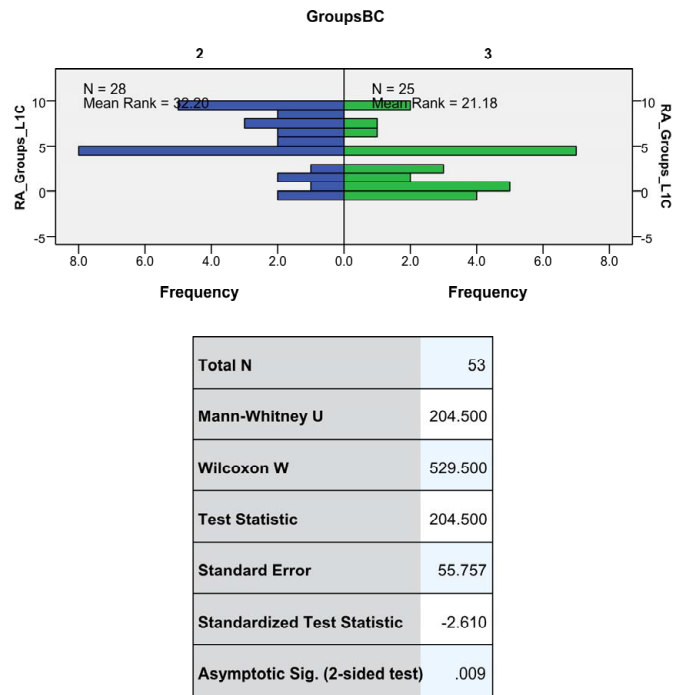
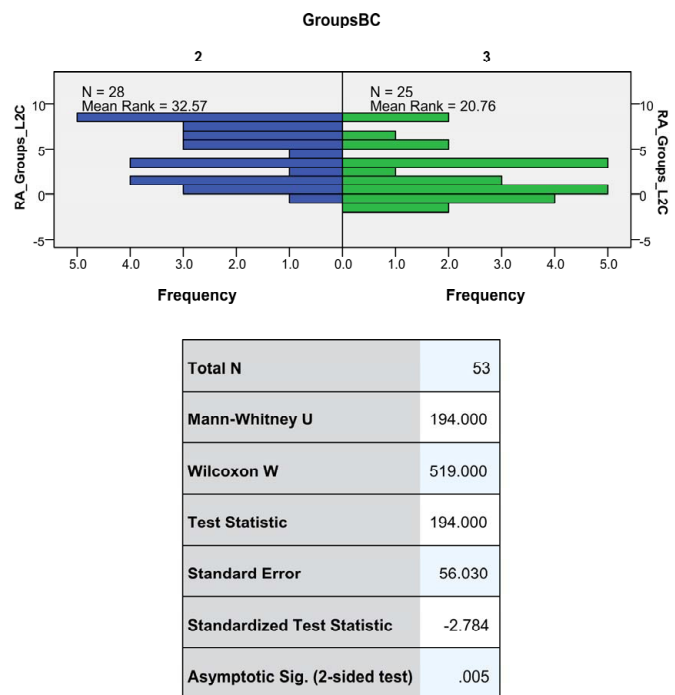
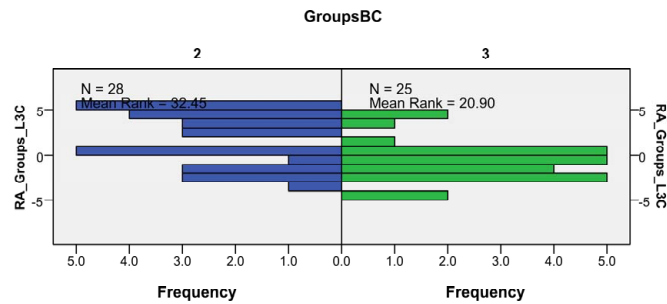


Figure 4.21: Mann-Whitney Test for Risk Aversion between Groups.



4.3 Analysis and Findings

Figure 4.22: Mann-Whitney Test for Risk Aversion between Groups.



Total N	53
Mann-Whitney U	197.500
Wilcoxon W	522.500
Test Statistic	197.500
Standard Error	56.012
Standardized Test Statistic	-2.723
Asymptotic Sig. (2-sided test)	.006

4.3.4 Four-fold Pattern of Risk Attitude

Finding 19: Information security professionals behave according to the four-fold pattern of risk attitude: they are risk-averse for small probabilities of loss and risk-seeking for large probabilities.

As we observe in Figures 4.23 and 4.24, professionals are risk-averse for small-probability levels ($p_1 = 0.05$ and $p_2 = 0.15$). Risk aversion gradually diminishes from level p_1 (first three lotteries in each figure) to p_2 (lotteries four to six), until it switches to risk-seeking behaviour (significant for some of the lotteries) at probability level $p_3 = 0.5$ (last three lotteries in the figures). The finding reproduces the prediction of prospect theory [90] for professionals, which we also detected in the experiment of Chapter 3.

Significance of risk aversion in WTP for the lotteries is measured with the parametric one-sample t-test on the “risk aversion variables”, and is presented in Table 4.7 for both abstract and scenario lotteries. The test determines whether the sample belongs to a population of a specific mean, with the mean in our case being the test value zero, which would be the choice of risk neutral decision-makers. The statistical requirements for the parametric test are met. Namely, the dependent variable is measured at least at interval level, data is independent (i.e. between-subjects), significant outliers are of restricted number and, finally, distribution of the dependent variable is approximately

4.3 Analysis and Findings

normal.

Figure 4.23: Mean risk-averse (positive) and risk-taking (negative) WTP of Professionals per Abstract Lottery. Bars represent participants' mean WTP minus the $\Delta(\text{Expected Value})$ between initial and modified lotteries.

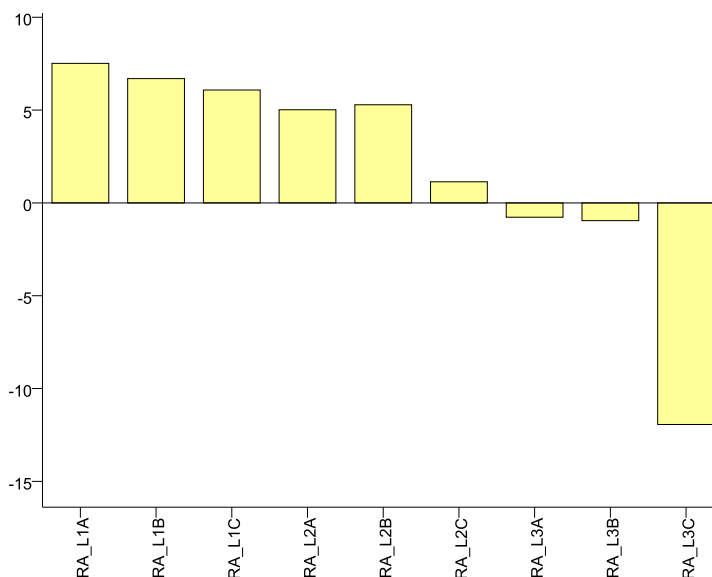
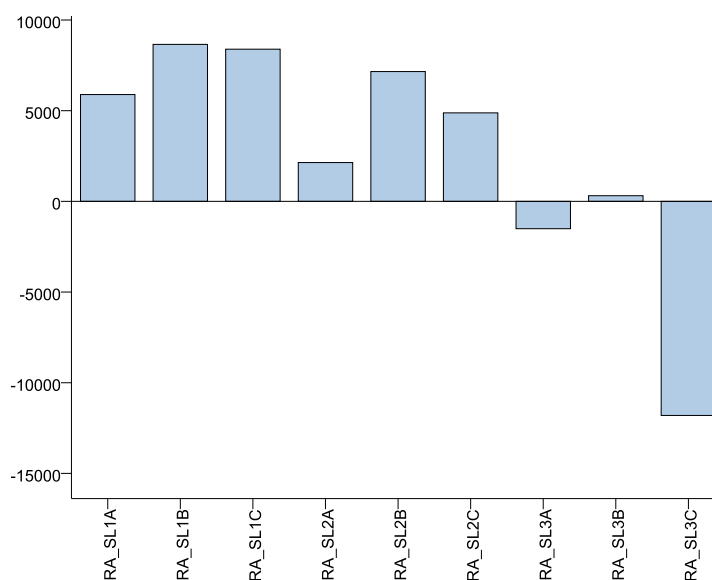


Figure 4.24: Mean risk-averse (positive) and risk-taking (negative) WTP of Professionals per Scenario Lottery. Bars represent participants' mean WTP minus the $\Delta(\text{Expected Value})$ between initial and modified lotteries.



It is noteworthy that the pattern also persists in the group-lotteries of the previous hypothesis (Table 4.6), including lotteries with high-probability gains, although presentation order of these lotteries was not randomised.

4.3 Analysis and Findings

Table 4.6: Mean differences of risk aversion values $RA_Groups_L_i$ from test value zero with the one-sample t-test ($TestValue = 0$, $N = 78$).

Group Lotteries (Unified Variables) ($N = 78$)				
Lottery	ΔEV	μ difference	95%CI of difference	
			Lower	Upper
$RA_Groups_L_1A$.25	2.30***	1.72	2.87
$RA_Groups_L_1B$.25	2.52***	1.99	3.04
$RA_Groups_L_1C$.5	3.24***	2.47	4.02
$RA_Groups_L_2A$.75	1.80***	1.22	2.37
$RA_Groups_L_2B$.75	1.87***	1.41	2.32
$RA_Groups_L_2C$	1.5	2.42	1.65	3.19
$RA_Groups_L_3A$	2.5	.38	-.08	.85
$RA_Groups_L_3B$	2.5	.55*	.08	1.01
$RA_Groups_L_3C$	5	-.67	-1.38	.02

* $p \leq 0.05$, *** $p \leq 0.001$

Table 4.7: Mean differences of risk aversion values RA_L_i and RA_SL_i from test value zero with the one-sample t-test ($TestValue = 0$, $N = 78$).

Experiment (Abstract) Lotteries L_{ij} ($N = 78$)				
Lottery	ΔEV	μ difference	95%CI of difference	
			Lower	Upper
RA_L_1A	1.25	7.52***	5.06	9.97
RA_L_1B	1.25	6.69***	4.99	8.39
RA_L_1C	2.5	6.08***	3.43	8.73
RA_L_2A	3.75	5.02***	2.56	7.47
RA_L_2B	3.75	5.28***	3.58	6.99
RA_L_2C	7.5	1.14	-1.12	3.39
RA_L_3A	12.5	-.77	-2.68	1.14
RA_L_3B	12.5	-.95	-2.76	.86
RA_L_3C	25	-11.93***	-14.35	-9.51

Survey (Scenario) Lotteries SL_{ij} ($N = 78$)				
Lottery	ΔEV	μ difference	95%CI of difference	
			Lower	Upper
RA_SL_1A	1,875	5,890***	3,899	7,880
RA_SL_1B	1,875	8,659***	6,296	11,022
RA_SL_1C	3,750	8,391***	5,217	11,565
RA_SL_2A	5,625	2,140*	149	4,130
RA_SL_2B	5,625	7,158***	4,505	9,810
RA_SL_2C	1,1250	4,882**	1,459	8,304
RA_SL_3A	18,750	-1,509	-4,158	1,139
RA_SL_3B	18,750	313	-2,944	3,570
RA_SL_3C	37,500	-11,807***	-15,220	-8,394

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

4.4 Discussion

In risk management there is no standard procedure for treating risk and decisions very often depend on the subjective judgement of the decision-maker. The scope of this study was to examine risk behaviour of information security professionals with regards to risk treatment and risk communication.

In the results of the first hypothesis regarding preferences amongst risk treatment actions, we observe that professionals preferred to reduce risk rather than eliminate it. These two choices are related to the risk treatment actions of *risk modification* and *risk transfer* (purchasing insurance), respectively. In the case of insurance purchasing, risk is transferred to another party. This preference was unexpected as eliminating risk completely should have an amplifying effect on professionals' risk aversion. Perhaps preference for risk modification is related to professionals' roles. It is, generally speaking, their job to modify risk by proposing and implementing security measures, not transfer it to some other party. It might be the case that many security professionals see the very existence of their role as one of modification of risk.

Another possible interpretation of this result is that professionals diminish the benefits of transferring risk because they feel that risk cannot be completely eliminated. In addition, there might be a sense of uncertainty and lack of control in professionals' perception when they place security in somebody else's hands. It would be interesting to examine the effect of "having control of your own risk" on professional's risk perception. This finding implies that professionals could be inclined to invest in security measures, even in situations in which buying insurance would be a more optimal solution in terms of expected returns.

In the second hypothesis we measured differences in WTP between reduction of probabilities and reduction of losses in risky lotteries. The results revealed significant differences between these two actions, in favour of losses reduction. This finding was also unexpected, as previous literature suggests that probability, as a value between zero and one, can be more easily "mapped" in the decision-maker's perception as "good or bad", which is not true for arbitrary outcome values. Thus, decision-makers can more easily characterise probabilities rather than outcomes as preferable or not [140]. However, effects were traced only in lotteries which were presented to the professionals as information security scenarios. This implies that professionals do not reveal such a bias in abstract lotteries, but it was the information security scenarios in which they changed their risk attitude. This means there must be context-related factors which cause preference for loss reduction.

Moreover, significant effects hold for realistically small and moderate probability levels

4.4 Discussion

only ($p_1 = 0.05$ and $p_2 = 0.15$). This result might have relevance to the debate between *proactive* and *reactive* security. Namely, measures that reduce probability of loss, i.e. vulnerability, effectively minimise the exposure of an asset to a threat and are therefore proactive. Reactive measures, on the other hand, focus on containing the damage caused *after* a threat has materialised. Reactive security is constantly attracting attention in the industry [144] and academia [23], as there appears to be a general consensus that both preventive and detective measures should be implemented. Another explanation for the manifested preference for loss reduction could be that professionals consider security breaches inevitable. Such an argument is reinforced by findings on increased WTP for avoiding small probability lotteries, in the experiment of Chapter 3. It could be the case that small losses are perceived as inevitable by professionals and that this leads to amplified risk aversion as well as a tendency to adopt a reactive approach to security. Therefore, professionals could be dispositioned to spend more on business continuity or disaster recovery measures, rather than reducing vulnerabilities.

The third hypothesis targeted different forms of risk framing. Three framing groups were used: losses, gains and a mixture with a step-by-step loss-framing. Findings did not reveal differences in the risk reduction variables amongst the groups. However, variables that measure WTP for avoiding lotteries were all found to be significantly different amongst groups. This difference is two-fold. Firstly, risk aversion is significantly larger for the gain-framing group, compared to the loss-framing group. These results are related to either the *possibility effect* or the *certainty effect* [90]. In the case of gains (Group B), the large probabilities of gaining (0.95, 0.85 and 0.5) accounted for professionals' fear of disappointment, fearing they would win nothing instead of securing the gains. So, they stated increased willingness to pay to secure lottery outcomes (certainty effect). In the case of losses (Groups A and C), the probabilities of loss (0.05, 0.15 and 0.5) also accounted for professionals' fear of disappointment, fearing they would lose something instead of securing a zero loss (possibility effect).

Findings indicate that the certainty effect for gains causes professionals to underweight very probable gains relatively to certain gains. The possibility effect for losses causes professionals to overweight unlikely losses. What was found is that the former underestimation is larger than the latter overestimation, in absolute terms. Thus, distortion of risk perception in the process of changing risk probabilities for either securing gains or avoiding losses is larger for gains than losses. In this sense, findings comply with prospect theory and, in particular, with risk behaviour across the probability ranges of the four-fold pattern [87]. Additionally, findings allow for a comparison between the magnitude of perceived probability distortion for large-probability gains and small-probability losses. In any case, such risk perception constitutes a violation of expected value maximisation, a fact which should be a concern in risk management.

4.4 Discussion

However, information security can be viewed in two ways: either as a necessary cost, i.e. a costly process with zero return, or as a business enabling operation with return on investment. Findings imply that professionals would be more risk-averse and would invest more in the second case.

The second interesting result in this hypothesis is that WTP for transferring risk is significantly larger in the step-by-step loss-framing group than in the loss-framing group. In the former group we rewarded participants with a monetary amount of \$10 before each lottery choice. In the latter, we gave them \$30 initially, and then presented them with the same three lotteries. Per-lottery payment made professionals more risk-averse, whereas they were less risk-averse when they were given the whole amount upfront. Actions of professionals on risk modification were not diversified by framing, but risk aversion was diversified in risk elimination. So, framing does not have effects on attitude towards risk reduction, but it affects perception when paying to eliminate risk.

A potential extension of this design in the real world could be a variation in budget allocation. For example, security professionals could be supplied with their entire budget from the start, or they could receive a per-project budget. If we were to hypothetically extend our conclusions, professionals would be significantly more risk-averse in eliminating risks by per-project budget allocation. A possible explanation is that the individual's attention on available budget becomes stronger if budget allocation is more frequent, in contrast to a single initial allocation. Thus, such a budget setting would make professionals spend more on insurance as a security investment.

The manifestation of risk aversion in professionals' decisions underlies the whole experiment. We reproduced the so-called four-fold pattern of risk attitude for losses [90], as subjects are found to be risk-averse for small probabilities of loss and become risk-seeking for large probabilities. This pattern is observed in both abstract and scenario-type lotteries, as well as in the group lotteries. Observations also confirmed increased risk aversion for high-probability gains in the group-lotteries. So, for realistic small (to moderate) probabilities of security breaches, we expect professionals to act in a predictably risk-averse manner, by investing more on security measures than the estimated expected loss. However, risk-taking behaviour for large-probability losses implies that professionals are willing to *accept* risk and this might be an issue of concern.

4.5 Summary

In this chapter we presented an experiment and survey for the purposes of studying the behaviour of information security professionals in tasks related with treatment of risk, after it has been assessed.

We examined preferences amongst equally-beneficial risk treatment actions. We also explored potential preferences towards probability- or outcome-reduction, given negative-outcome lotteries. We framed identical problems as gains and losses and we created experiment conditions in which losses were either extracted from a single budget or from individual budgets. We also measured the overall attitude towards risk, for various levels of probabilities and outcomes.

Findings revealed that professionals prefer to take action towards modifying risk, rather than transferring risk to another party. They also showed a preference for outcome reduction instead of probability reduction, in risk modification. The prospect of eliminating risk completely, does not have an effect on professionals' risk attitude. Budget allocation has a significant influence in professionals' risk behaviour making them more risk-averse when provided with separate budgets. Presenting security problems as gains, instead of losses, also increases professionals' risk aversion significantly. Professionals are observed to be risk-averse in small-probability and low-impact lotteries and become risk-seeking as stakes increase.

As a conclusion, professionals reveal characteristic preferences for treating risk. Most importantly, their risk attitude is influenced by the presentation of security problems, like viewing security as a loss or a gain, or allocating budget differently. These findings indicate that except for individual risk attitude, there are decision points inherent in risk management that can influence decision-making in information security.

Implications

Contents

5.1	Summary of Findings	129
5.2	Supplementary Survey	130
5.3	Survey Findings	130
5.4	Semi-structured Interviews	139
5.4.1	Interview with David Brewer	139
5.4.2	Interview with Paul Dorey	142
5.4.3	Interview with Bruce Schneier	145
5.5	Discussion on Implications	146
5.5.1	Risk Aversion and Ambiguity Aversion	146
5.5.2	Performance of Professionals and Students	148
5.5.3	Professional Roles	149
5.5.4	Proactive vs Reactive Security	150
5.5.5	Framing	151
5.5.6	Perception	152
5.5.7	Communication	154
5.5.8	De-biasing Decisions	155
5.5.9	Discussion on Recommendations	156
5.5.10	Summary	158

In this Chapter we summarise experimental results, we further examine risk perception of professionals via a survey, and we explore the significance of research findings by interviewing information security experts.

The Chapter is organised in the following way. The most important findings of the previous experiments are presented in Section 5.1. We conduct a supplementary survey, which examines additional aspects of information security professionals' perception of risk. A description of the survey and the analysis of its findings are presented in Sections 5.2 and 5.3. The full details of the survey are provided in Appendix A.4.0.1.

5.1 Summary of Findings

We interview three information security experts and ask them for their view on the importance and consequences of the research findings. The interviews are presented in Section 5.4.

We discuss the implications of our research findings in Section 5.5. Finally, we provide a number of recommendations for organisations, for the purposes of minimising the manifestation of observed biases and moderating deviations from expected value maximisation in decision-making.

5.1 Summary of Findings

A summary of the most important findings of the aforementioned two experiments is presented in a condensed fashion in this section. These findings were presented and discussed with renowned experts in information security both from the industry and academia (see Section 5.4).

Finding 1: Both information security professionals and students behave according to prospect theory: they are risk-averse for small probabilities of loss ($p_1 = 0.05$ and $p_2 = 0.15$) and risk-seeking for large probabilities ($p_3 = 0.5$).

Finding 2: Information security professionals reveal ambiguity aversion in their choices.

Finding 3: Information security professionals deviate less from expected value maximisation than the student sample.

Finding 4: Information security professionals exhibit preference inconsistencies between willingness to pay and choice decisions and reveal different risk attitudes to the ones they self-report.

Finding 5: Information security professionals have significantly different preferences for either security or operational time; these preferences are to a great extent dependent on their job role. Professionals are loss averse in their preferred attribute (security or operational time).

5.2 Supplementary Survey

Finding 6: The possibility of eliminating risk by paying does not have an additional effect on professionals' risk attitude. Information security professionals reveal a preference for paying to reduce risk compared to paying to eliminate risk.

Finding 7: Information security professionals reveal a preference for reducing losses instead of reducing the probabilities associated with these losses, in threat scenarios.

5.2 Supplementary Survey

A short supplementary survey was conducted by contacting information security professionals who are current and past students of the masters program in Information Security at Royal Holloway University of London. The purpose of the survey is to get more detailed responses on the perception of professionals on various risk-related aspects of information security. Participants took part in the survey online, from 5/09/2016 to 19/09/2016 and were presented with a series of questions that we discuss in Section 5.3.

All survey questions can be found in Appendix A.4.0.1.

5.3 Survey Findings

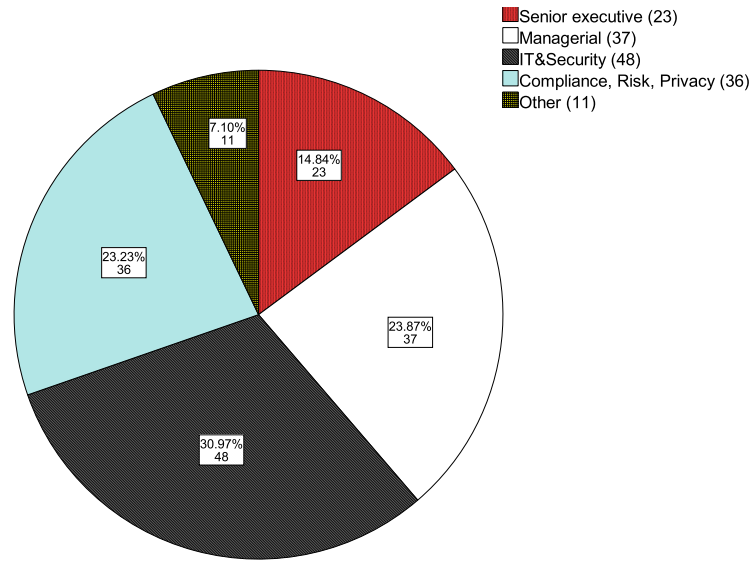
This survey was conducted for the purpose of better understanding risk perception of security professionals regarding their personal attitude, as well as the attitude of their colleagues and other security professionals. The survey was answered by 155 information security professionals and practitioners; five participants stated that they are not related to information security and were removed from the sample.

Participants were asked to choose the security role which most closely matches their current or past job position (Figure 5.1); we assign roles in four broad categories, as in the previous surveys, along with an additional category "Other", which allows participants to state a different position.

One of the survey questions refers to a choice between two same-expected-loss gambles. The first gamble involves a probability of loss twice as large as the second gamble, whereas the second gamble has a loss that is two times the loss of the first gamble (Figure 5.2). Based on the previous experiments, the expectation would be that

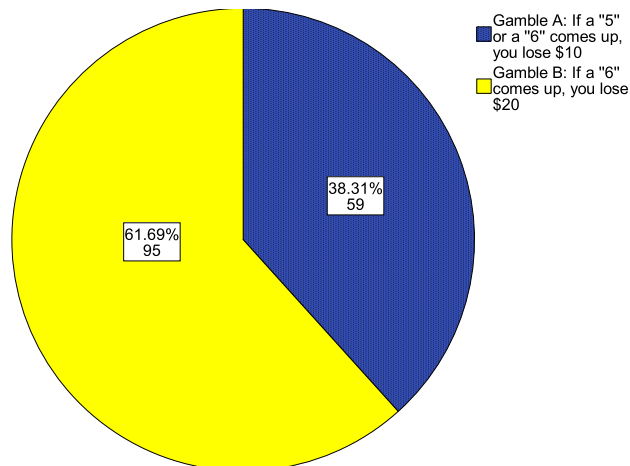
5.3 Survey Findings

Figure 5.1: “Your current or last job role most closely resembles:”



professionals prefer the gamble with the minimum losses, as this was the statistically significant choice elicited in 4.3.2. The majority of participants (about 62%), chose the gamble with the lower probability of loss, which indicates a context-relation of Section 4.3.2 findings.¹

Figure 5.2: “Which one of the following gambles do you instinctively prefer, at first glance?”



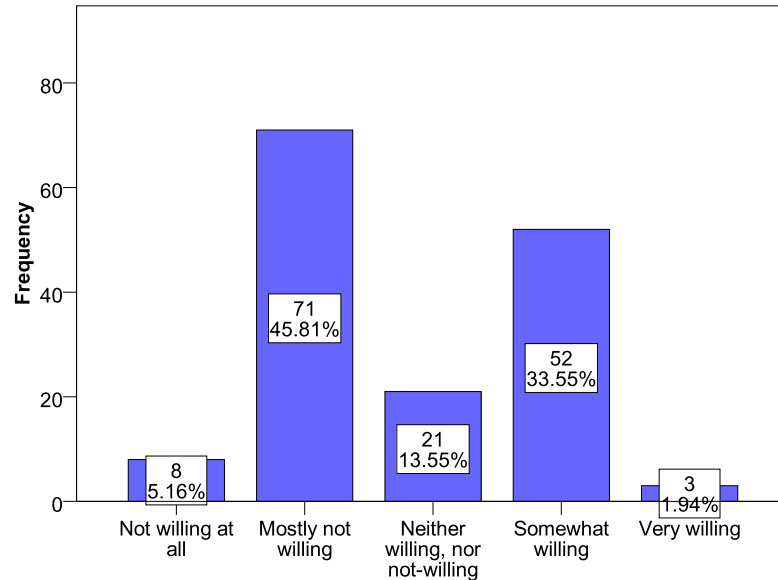
Professionals' perception of risk is elicited via five risk-related survey questions in which participants had to choose their replies from a Likert scale ranging from one to five. The first question regards professionals' perception on the risk attitude of other security professionals (Figure 5.3). We observe that the majority of professionals consider other

¹Experiment results of Section 4.3.2 did not reveal significant preferences of professionals between probability and negative outcome reduction, in abstract lotteries, but only in information-security-scenario questions.

5.3 Survey Findings

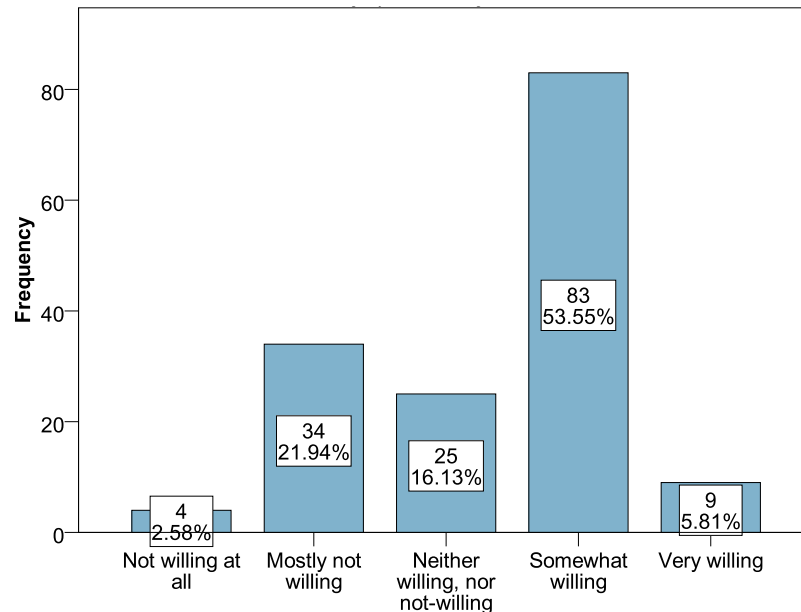
professionals as slightly risk-averse ($\mu = 2.81$, with value 3 denoting neutrality).

Figure 5.3: “In your opinion, how willing are Information Security Professionals to take risks in general?”



The majority of professionals report themselves as being risk-seeking with $\mu = 3.38$ (Figure 5.4).

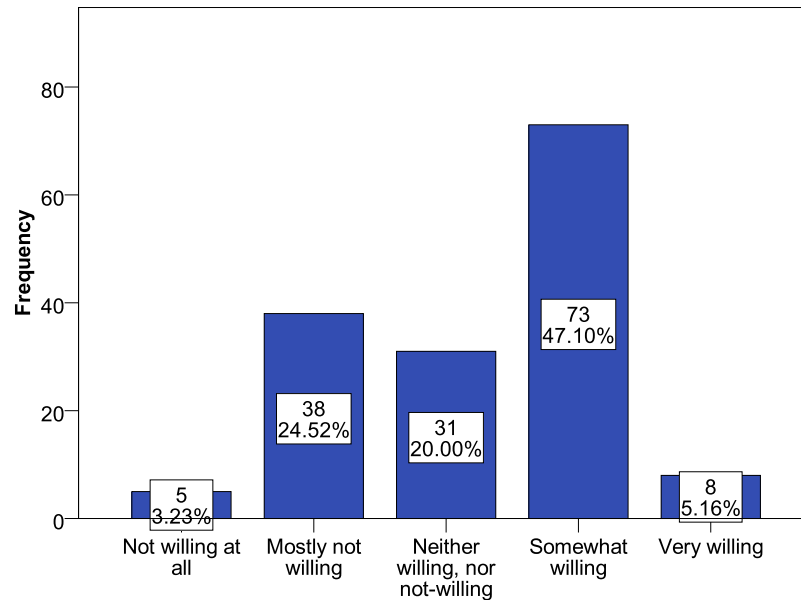
Figure 5.4: “How willing are you to take risks in general?”



A similar risk-taking attitude is observed in professionals' risk attitude in the context of their information security role with $\mu = 3.26$ (Figure 5.5).

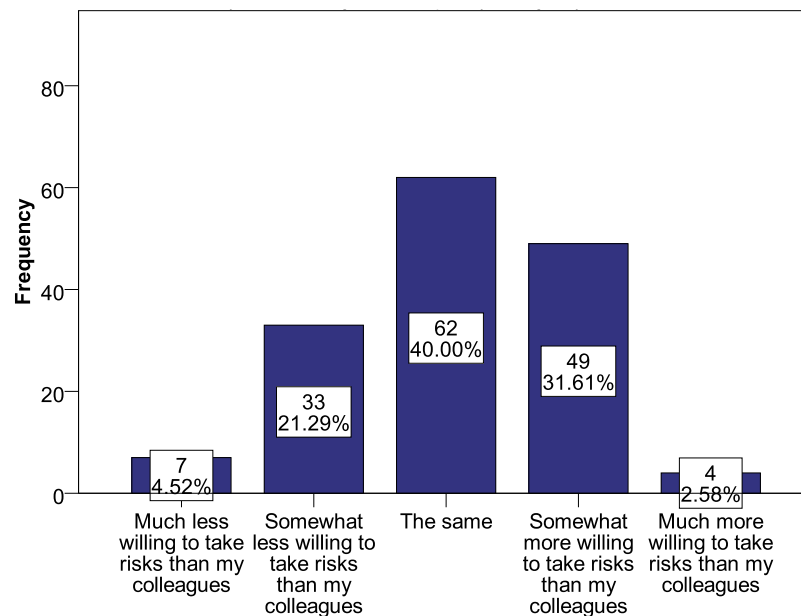
5.3 Survey Findings

Figure 5.5: “How willing are you to take risks in your [] role?”



In comparison to their colleagues, professionals believe that they are slightly more risk taking than their colleagues with $\mu = 3.06$ (Figure 5.6).

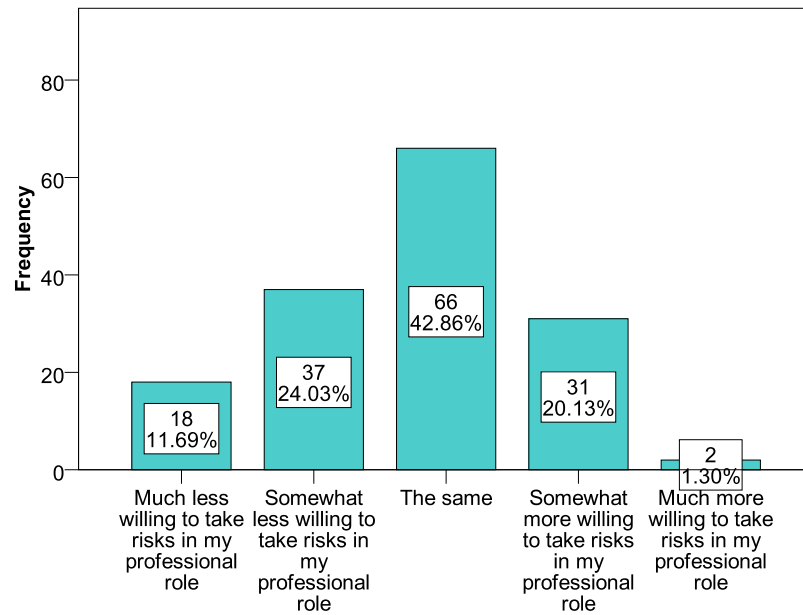
Figure 5.6: “Are you less or more willing to take risks compared to your colleagues in your [] role?”



Finally, professionals report that they are more risk-averse in their job roles than in their personal lives with $\mu = 2.75$ (Figure 5.7).

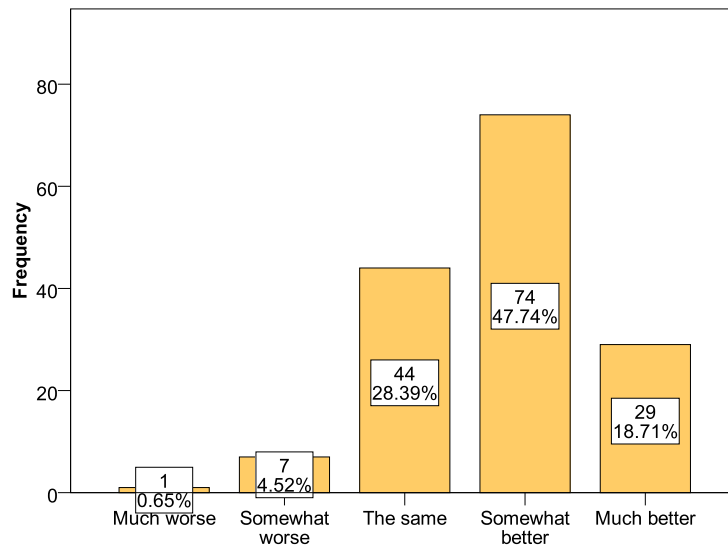
5.3 Survey Findings

Figure 5.7: “Are you less or more willing to take risks in your [] role than in your personal life?”



Professionals perceive themselves as somewhat better in their mathematical skills compared to the general population; $\mu = 3.79$ (Figure 5.8).

Figure 5.8: “Do you think that your mathematical abilities are worse or better than the average person’s in the general population? (E.g. with respect to probabilities and expected values)”



The next questions depict the perception of professionals on the prioritisation of either security or operational time, amongst the various roles of security professionals. We observe a clear dichotomy in perceptions indicating that security is perceived as a priority for IT and security related professionals as well as for compliance, risk and

5.3 Survey Findings

privacy related professionals (Figure 5.9). Prioritisation of operational time is perceived as a characteristic of senior executive and managerial roles (Figure 5.10).²

Figure 5.9: “In your opinion, which of the two attributes: Security or Operational Time, is perceived as more important by the following professional roles?” (Participants that chose “Security”)

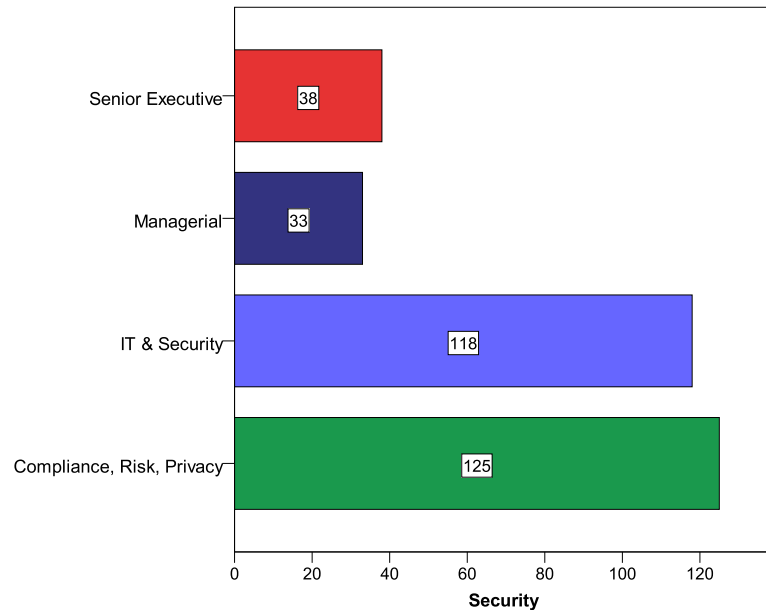
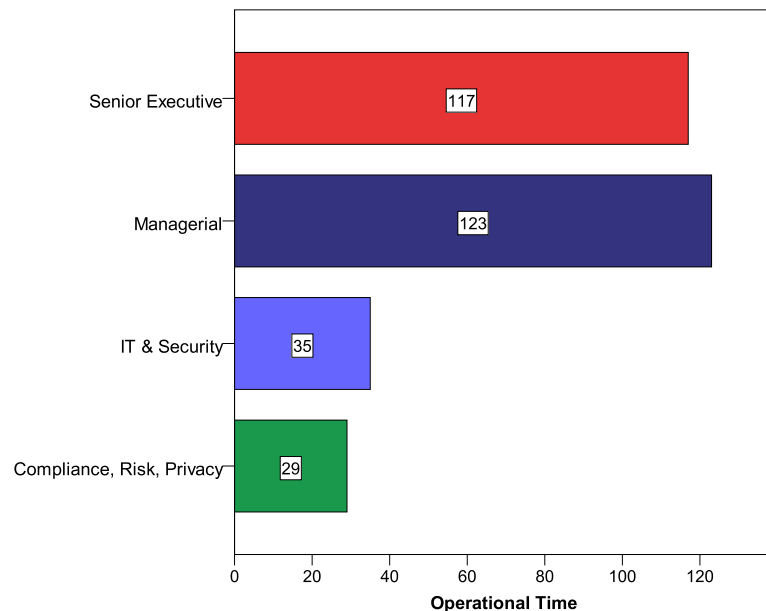


Figure 5.10: “In your opinion, which of the two attributes: Security or Operational Time, is perceived as more important by the following professional roles?” (Participants that chose “Operational Time”)



²Security roles, when examined separately, do not reveal statistically significant differences on perceived importance of security or operational time (Pearson’s Chi-Square, Likelihood Ratio and Linear-by-Linear Association tests).

5.3 Survey Findings

This self-reported perception contradicts previous experimentally elicited findings on the preference between security and operational time. Namely, in Experiment 1 senior executives as well as compliance-related professionals reveal a preference for security, managers prefer operational time and IT & security professionals are divided amongst the two attributes (3.6).

Professionals reveal the following prioritisation for 11 criteria that were presented to them in two settings. In the first setting they are asked to classify and rank their preferred criteria as important and less important in a hypothetical scenario. In the second case they are faced with the same task, but in the context of their job role. In Figures 5.11 and 5.12 criteria which correspond to odd numbers are priorities and criteria that correspond to even numbers are the choices of secondary importance.

The list of the 11 criteria is presented here:

1. Estimating expected losses, e.g. $\text{Asset Value} \times \text{Vulnerability} \times \text{Threat Probability}$
2. Considering losses of the worst-case scenario
3. Estimating a specific probability of loss instead of a range of probabilities
4. Prioritising security of the system
5. Prioritising operational time of tasks
6. Investing in security measures for small-probability threats
7. Investing in security measures for large-probability threats
8. Eliminating existing risk completely
9. Containing potential losses in case of a security incident
10. Reducing the vulnerabilities of the system
11. Obtaining appropriate insurance

There is a significant difference in the ranking of criteria between the hypothetical scenario and the job role-dependent prioritisation per participant, per criterion that is considered as a priority and per criterion that is considered as of having secondary importance (Table 5.1).

5.3 Survey Findings

Figure 5.11: “Imagine you are responsible for the Information Security budget; you have to consider potential information security threats and take an approach for protecting assets to an optimal level. Evaluate and rank the following decision criteria in two groups: the most important decision criteria and the criteria of secondary importance:”

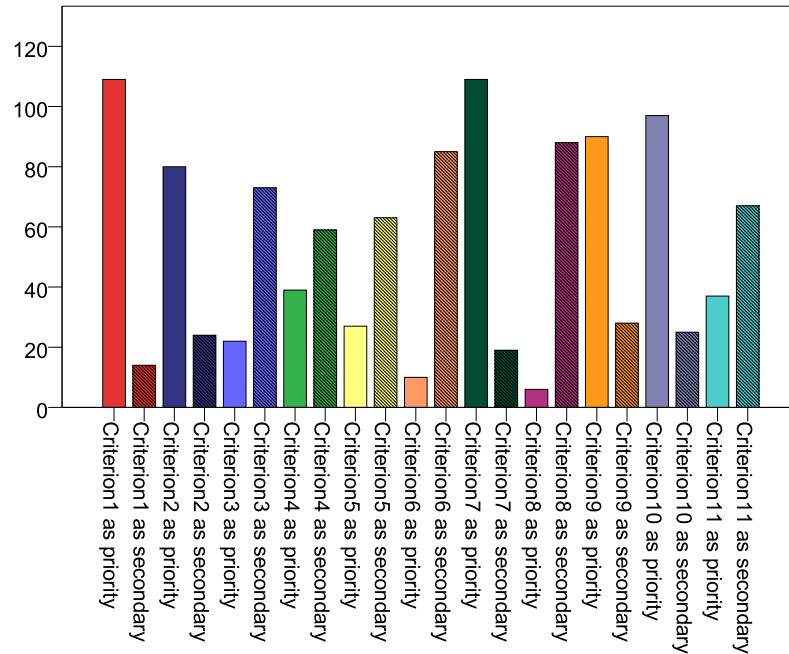
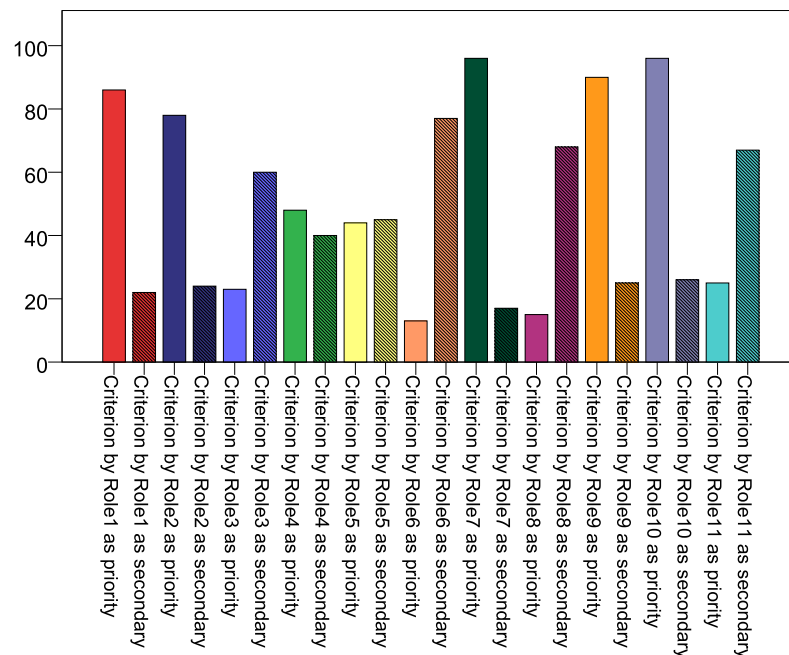


Figure 5.12: “Which of the following decision criteria, for protecting assets to an optimal level, do you think that you are mostly focused on or worried about as a result of your [] role?”



5.3 Survey Findings

Table 5.1: Wilcoxon Signed Ranks Test for pairwise comparisons of decision criteria between hypothetical scenarios and professional-role questions.

Wilcoxon Signed Ranks Test			
#	Criterion	Prioritisation	Statistic
1	Estimating expected losses	priority	-3.592 ^{b***}
		of secondary importance	-1.706 ^c
2	Considering losses of the worst-case scenario	priority	-.378 ^b
		of secondary importance	.000 ^a
3	Estimating a specific probability of loss	priority	-.243 ^c
		of secondary importance	-2.502 ^{b*}
4	Prioritising security of the system	priority	-1.800 ^c
		of secondary importance	-3.307 ^{b**}
5	Prioritising operational time of tasks	priority	-3.053 ^{c**}
		of secondary importance	-3.087 ^{b**}
6	Investing in security measures for small-probability threats	priority	-.728 ^c
		of secondary importance	-1.512 ^b
7	Investing in security measures for large-probability threats	priority	-2.414 ^{b*}
		of secondary importance	-.408 ^b
8	Eliminating existing risk completely	priority	-2.714 ^{c**}
		of secondary importance	-3.922 ^{b***}
9	Containing potential losses in case of a security incident	priority	.000 ^a
		of secondary importance	-.577 ^b
10	Reducing the vulnerabilities of the system	priority	-.192 ^b
		of secondary importance	-.192 ^c
11	Obtaining appropriate insurance	priority	-2.268 ^{b*}
		of secondary importance	.000 ^a

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

a. The sum of negative ranks equals the sum of positive ranks.

b. Based on positive ranks.

c. Based on negative ranks.

5.4 Semi-structured Interviews

Three highly experienced individuals in information security were contacted and presented with the experimental approach, the design and the specific findings. A semi-structured interview was conducted with each of the three experts during which they were asked about their views and opinions on the importance and the potential implications of the findings. The following questions were presented to and discussed with the interviewees; however, the interviews allowed for a broader discussion on risk management, behavioural issues and decision-making in information security.

Interview question 1: Did you find any of the findings surprising? If so, please indicate why.

Interview question 2: According to ISO 27005 *risk perception* and *risk attitude* are factors that need to be taken into consideration in current information security risk management methodologies.

- To what extent do you think individual *risk perception* and *risk attitude* of information security professionals is an important factor in decision-making?
- How important do you think these factors are for making decisions regarding *risk treatment*?
- How can we address this issue in your opinion?

Interview question 3: What do you think the potential implications of these findings are? How can organisations benefit from these findings?

Interview question 4: Which aspects of decision-making in information security do you think need to be further examined?

5.4.1 Interview with David Brewer

Dr. David Brewer was one of the first consultants to advise the British Government on information security matters, providing assistance to establish the first ever computer security evaluation facilities and evaluation criteria. He was a founder member of the Department of Trade and Industry's Commercial Computer Security Centre (1987-1992) and became a co-author of the European IT Security Evaluation Criteria (the forerunner of ISO/IEC 15408) and associated evaluation manual and a co-author of the original ISMS standard, BS 7799 Part 2. He is now an active member of the UK delegation to ISO JTC1 SC27 WG1, which is responsible for the ISO 27000 family of

5.4 Semi-structured Interviews

standards; and is co-editor for the revision of ISO/IEC 27004 (Measurements). He has conducted a wide variety of consultancy assignments in information security spanning 32 years in over 23 countries. He is well known for his work in rolling out ISO/IEC 27001 to the whole of the Civil Service in Mauritius, which is an exemplar of his ISMS implementation methodology, and his ability to train people to train others. His seminal research papers include The Chinese Wall Security Policy, published in 1989 [36] and Measuring the Effectiveness of an Internal Control System, published in 2003 [35].

Risk ownership

During our interview (28/08/2016) David's first remark was the distinction between an asset owner and a risk owner. Indeed, this aspect has been emphasised in the ISO 27001 changes, from the 2005 to the 2013 edition [37]. Although assigning asset owners is a means for assigning responsibility for an asset, a risk owner is a "person or entity with the accountability and authority to manage a risk". This person, and it should preferably be a person rather than an entity, needs to have an incentive to resolve risk and also needs to be positioned high enough in an organisation to be able to act. So, David highlighted that the diversification of incentives between risk owners and other professionals is vital in the risk management process. The main reason is the responsibility of risk owners in accepting any residual risk. In our research we approached a wide range of information security professionals, including risk owners, as we wanted to examine risk perception across various roles.

Probabilities vs Outcomes

The research finding in which professionals reveal a preference for minimising consequences (losses) instead of probabilities was welcomed by David. As he stated, this is the way to think about a potential threat, i.e. what the potential impact of a threat is. This mindset is important because when a decision is to be made, the consequences are discussed and the risk appetite is examined based on these consequences. The reason is that the actual probabilities associated with the threat at hand are most likely unknown. David pointed out that after the 9/11 incidents some business continuity plans worked exactly because they were not based on specific, and quite unpredictable, events, but on consequences and on the severity of these consequences.

Subjective Perceptions

Regarding the existence of biases in decision-making, David recognises that biases are inherent in the process. He mentioned an example of physical security, namely a scenario in which a laptop is snatched from its owner. Retrospectively, after the theft, the decision-makers might want to analyse what they would have done differently in order to avoid the incident. They might change their plan, for example, use a backpack instead

5.4 Semi-structured Interviews

of holding the laptop, or have someone else carry the laptop next time. So, firstly, it is the consequence, the theft itself, that is taken into consideration, not the likelihood of the the event. Secondly, the bias in this case is that “our view of the consequences changes” for a variety of reasons (here due to experiencing the theft incident), but the actual consequences do not change. Thus, we would protect ourselves more *after* this unpleasant experience, but, we would possibly not take adequate measures beforehand. So, subjective views can be considered inherent in the process of learning and improving risk management.

Imitating and Learning

David argued that a typical phenomenon in information security is learning from your “neighbours”, i.e. from watching the measures that competitors or organisations of similar nature take, or even from observing breaches and losses that others suffer. Indeed, an educated decision needs to be made by each organisation on whether to follow other approaches or to stick to its own plan. This point was interestingly also mentioned by the next interviewee.

Business Orientation

One of the main points that David made was the importance of the business part of an organisation. It is the business objectives that the focus is on. In other words, the stakeholders make decisions on ceasing or creating opportunities to meet these business objectives. Some of the dangers associated with these decisions are information security-related, and have to be dealt with. So, information security risk management depends on business exploitations. In this sense, information security is not the epicentre of importance but business objectives are. From this point of view, David argued that it would be interesting to further examine the link between information security and business objectives. In particular, it would be useful to examine the ability to connect security needs to business and consequently to inform risk owners.

Risk Communication

David also agreed that the opinion and recommendations of security professionals are important. From his own experience he highly values an effective way of communication between security and business people. In order for this communication to be effective, David proposed that security professionals should convey their message as if “telling a story”. This “tell it like a story” approach is probably another argument for the decision-makers lack of understanding in probabilities and outcomes, and by this approach both parties can effectively share the same “decision context”. It is the simple storyline of an unwanted consequence that we want to achieve and David’s approach highlights this. This might be a straightforward and effective way to bridge the gap between the

5.4 Semi-structured Interviews

security and the business point of view.

5.4.2 Interview with Paul Dorey

Professor Paul Dorey (Ph.D. CISM F.Inst. ISP) is a visiting professor in Information Security at Royal Holloway, University of London, Chairman Emeritus at the Institute of Information Security Professionals, a former CISO BP PLC and Group Operational Risk Director at Barclays Bank. Paul has over 30 years management experience in information security and is an acknowledged thought leader. He has received several industry awards including Chief Security Officer of the Year, IT Security Executive of the Year, and IT Security Hall of Fame. He now acts as a lecturer, consultant and expert witness and is helping major companies and government departments devise their cybersecurity strategies and future risk management, measurement and reporting approaches. His recent project work includes developing strategies in managing the security of the “Internet of Things” (www.trustedthings.com) and how executives, engineers and IT teams will need to work together in new ways.

Probabilities vs Outcomes

In our interview (12/09/2016) Paul found the observed preference of professionals towards loss (impact) reduction compared to probability of loss (vulnerability) reduction very logical and indeed, understandable. Paul argued that this is what security professionals are trained to do: reduce the potentially worst-case negative impacts.

Influence of Security Professionals

We explained during the interview that we realise that the security professionals who participated in the research are not necessarily those who make the final call in the decision-making process, i.e. they are not necessarily the risk owners. Paul’s reply very much coincides with our own reasoning behind this design choice. He mentioned a personal story from his early career as an information security officer in which he expressed the same consideration to a senior executive, i.e. that he was not the person that made the final call in a security decision. The senior executive replied that the impact of the suggestions which security professionals make should not be underestimated; and this is the belief that Paul conveyed during our interview. In other words, the effect of these suggestions, albeit not the final decision, can directly or indirectly influence the decision at hand.

Influence by Fear

Another point related to this aspect is that, based on Paul’s experience, security professionals can attempt to influence decisions by fear. In information security environments,

5.4 Semi-structured Interviews

he reported that he has witnessed and very much disagrees with, an additional exaggeration on potential losses by a few security professionals, in their sometimes desperate attempt to obtain a larger budget. A relevant concern that Paul raised was that there could be other agendas on the professionals' mind when they consider various solutions. These agendas can include the ease of justification of professionals' choices, considerations about their career progression as credible managers, potentially lost opportunities and so on. It is noteworthy that behaviour of participants in our incentivised economic experiments coincides with their attitude in the information security scenario-based questions. In this sense, professionals acted in a similar fashion in almost all the abstract experiments and the surveys. Moreover, given our experimental findings, with the clear risk aversion of professionals towards low- and moderate-probability threats, we believe that the "influence by fear" approach, which would be an intentional behaviour, as well as the possible agendas considered by the professionals, would only amplify the risk averse behavioural trait that was observed.

De-biasing Decisions

Paul suggested that our research findings might help in de-biasing the process of decision-making in information security. More specifically, he believes that these findings show that to estimate the level of investment by adjusting risk perception is not the right way of doing it. So, professionals, should, when they can, try to get the most optimal risk perception they can, that is, eliminate biases from their own decisions, so that they make informed decisions. In an idealised view, security professionals would bring knowledge to the table for discussion with business people. This would, hopefully, allow for a common conclusion to be reached between the business and the security side, based on the given facts and not as an adversarial compromise between the two sides. So, in Paul's view information security should eventually rely more on data.

Risk Communication

Another important remark was that the aforementioned need for facts-driven decisions is that the final decision-maker is usually not fully aware of context and the role of the security expert is to describe this context objectively. Paul reported that it is not unusual for security professionals to have to intervene in a situation at the last minute, exactly because of this "lack of context" that the business-oriented decision-makers understandably exhibit.

Security - Operability trade-off

The diversification of preferences between security and operability (operational time) was welcomed as an interesting and realistic finding by Paul. He noted that the mindset, for example, of the most senior executives, which have the most broad view of the

5.4 Semi-structured Interviews

business, is inherently different to the view of project managers. Managers, in particular, very often fear small losses that senior executives are willing to accept. Yet the same managers may miss the importance of damaging strategic risks such as to reputation, which executives focus on immediately.

Risk Aversion

In Paul's view, one would expect security professionals to be very conservative, as they constantly worry with ideas of bad outcomes. Behaviour elicited in the experiments indeed shows that professionals are risk and ambiguity averse (except for large probability losses); however, survey findings report that only 24.52% of professionals consider themselves as risk-averse in general (Figure 5.4) and only 27.75% state that they are cautious and not willing to take risks in their professional roles (Figure 5.5).

Worst Scenarios

Another point that Paul made was regarding the worst scenario that he can think of in a security environment. His view is that this worst-case scenario would be a misplaced security investment, which can be worse than a non-investment, in some cases. For example, if a professional decides to invest a few million dollars on a specific system and a significant breach manifests on another system, the professional would regret his or her choice, as poor risk management.

Risk Seeking Behaviour

A hard-to-interpret research finding is the participants' shift towards risk seeking behaviour for large probability lotteries ($p = 0.5$) as in [90]. Paul expressed his puzzlement in interpreting this result from an information security perspective.

Imitating and Learning

In terms of other relevant interesting aspects of behaviour in information security, Paul believes that professionals, in general, like to "follow the crowd", particularly in the world of security solutions. For example, if there is a new technology that is trending in the field, then security programs will start adopting this technology on the basis of peer benchmarking and direction. It could be the case that there is a better non-trending solution which covers even more of the risks that the organisation has to defend against, but this latter solution would likely be neglected. Such a phenomenon of finding safety in the crowd might be related to the previously mentioned example of misplaced security investment. Following practices which other professionals adopt can be a way of justification, especially in the case of a materialised security incident, in the spirit of an "everybody does it" type of argument. Moreover, it is easier to justify a "commonly made" mistake, than justifying a mistake made by one individual.

5.4 Semi-structured Interviews

5.4.3 Interview with Bruce Schneier

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by The Economist. He is the author of 13 books, as well as hundreds of articles, essays, and academic papers. His influential newsletter “Crypto-Gram” and his blog “Schneier on Security” are read by over 250,000 people. He has testified before Congress, is a frequent guest on television and radio, has served on several government committees, and is regularly quoted in the press. Schneier is a fellow at the Berkman Klein Center for Internet & Society at Harvard University, a Lecturer in Public Policy at the Harvard Kennedy School, a board member of the Electronic Frontier Foundation, an Advisory Board Member of the Electronic Privacy Information Center, and the Chief Technology Officer at Resilient, an IBM Company.

Probabilities vs Outcomes

During our interview (16/09/2016) Bruce, similarly to the other interviewees, was positive towards the preference of professionals for reducing losses instead of reducing the probabilities associated with these losses. He believes that this might signify a conscious choice of resilience over defence. In his view such a choice indicates a reactive approach to security that is more sensible, because if the futility of prevention is recognised by information security professionals, then the next logical step is to focus their efforts on survivability, adaptability and resilience. In which case, probability reduction becomes a secondary issue.

Risk Behaviour and Risk Management

Bruce stated his concerns about generalising the research findings too much. However, he notes that this kind of research is demonstrating the need for taking risk perception and risk attitude into consideration in information security risk management. The observed deviations from perfectly rational behaviour and from expected losses minimisation reveal why risk attitude is important in the risk management process. What companies spend on, what they take seriously, and which factors they underestimate or overestimate, are all subject to these suboptimal decisions.

Bruce agrees that embedding risk perception and attitude into a risk management process is not an easy task. His view is that knowledge of the existence of potential biases on its own could significantly contribute to objectifying the decision-making process. As he points out, professionals should be aware of their own biases and be aware of their bounded rationality which determines their own “box of concern”, which is not necessarily the “larger box”. So, even the fact of understanding these biases could be incredibly valuable for making decisions. Bruce continued that in order to take advantage of these research findings we can try to correct the biases and inconsistencies

5.5 Discussion on Implications

as we would want organisational choices to be rational and we would want the level of security investment to be commensurate with the risks in ways that produce a maximum effect. These cognitive biases or inherent attitude towards risk are factors that we need to know about, so that we can correct them. Bruce gave an example of a security manager that moves into a new company. The manager should notice, for example, a uniform overspending or underspending on a security aspect. Such an inflation or undermining in spending is very likely to be caused by the belief structure of the individuals involved in decision-making. The security manager should be able to recognise the existence of such beliefs and subsequently to try to correct the investment approach.

Inconsistent Behaviour

The observed inconsistencies between decisions by choice and WTP were of interest to Bruce, especially the alignment of inconsistent behaviour between the professionals and the student sample; as he wittily phrased it: “inconsistencies were consistent” amongst the samples and this fact implies that there exists an underlying behavioural trait in the observations.

Bruce advocates that any research approach which focuses on biases and on how decision-makers deviate from optimality is worth investigating.

5.5 Discussion on Implications

5.5.1 Risk Aversion and Ambiguity Aversion

Risk Aversion

One prevalent finding which emerges in both experiments is the manifestation of the prospect theory pattern of risk attitude for the domain of losses. We observe that professionals, as well as students, are significantly risk-averse for small- and medium-probability losses and become risk-seeking for large-probability losses³. The pattern is similarly manifested both in lottery-type questions in which participants had to play with real money (Figures 3.2 and 4.23) and in hypothetical security investment scenarios (Figure 4.24). The first leg of this finding, i.e. risk aversion via overweighting small probability losses is explained by fear of disappointment in case an improbable event happens. The fear of *regretting* having not invested enough in protecting against a low probability threat makes individuals risk-averse. The second aspect of this finding, i.e.

³Compliance with prospect theory can be considered as not surprising, since it is an observational theory.

5.5 Discussion on Implications

risk taking behaviour for avoiding very probable losses is hard to interpret from an information security perspective, as all of the interviewees pointed out in Section 5.4. A threat probability of 0.5, which was used in our experiments, can be considered as “very probable” in information security. Based on prospect theory, consequences that are almost certain, or very likely, tend to be given less weight by the decision-maker, compared to the expected weight based on the associated probability. The fourfold pattern of risk attitude for the domain of losses (Table 2.2) implies that professionals *hope* to avoid losses when probability is high and thus become risk seeking. So, in the mind of professionals, investing large amounts for avoiding such a loss is very painful, hurting almost as much as the actual loss in the case of high probability threats. On the other hand, the opportunity to avoid the loss completely is appealing, so individuals systematically take risks in such lotteries. This implies that security incidents which are manageable, either by investing in security measures or by buying insurance, could turn into catastrophes, similarly to situations of desperate gambling. It is noteworthy that this risk taking effect is manifested for both risky and ambiguous lotteries.

However, significant risk aversion is also exhibited for small losses. This might imply that professionals do not want to take risks, especially for events which have little likelihood of occurring. So, they might justify expenditure for low-impact threats and they are willing to invest more to avoid them. It can be the case that small losses are considered as inevitable by professionals, and thus the associated investment is considered as unavoidable.

Risk-averse behaviour for small losses along with risk aversion for small probabilities and risk-seeking behaviour for large losses could result in over-investment in simple preventive measures for common information security threats (e.g. malware, viruses); but under-investment, as a willingness to accept some risk, in measures against potentially catastrophic breaches.

A simple means of controlling for risk aversion and risk-seeking behaviour in quantitative risk management approaches, is for information security professionals to take into consideration the difference between the investment amount and the expected losses, whenever information is sufficient. In case there are additional factors which influence the investment level, they need to be inserted in the estimation of expected losses.

Ambiguity Aversion

At the same time, professionals are found to be ambiguity averse, so that they are consistently willing to pay more than the expected loss of a threat, if losses are associated with a range of probabilities instead of specific probabilities. The same result holds for ranges of negative outcomes instead of fixed outcomes. Moreover, we observe the gradual increase in WTP as we change the exposure of professionals from risky to

5.5 Discussion on Implications

ambiguous and then to fully ambiguous lotteries, i.e. with ranges of both probabilities and outcomes (Table 4.7). Professionals' risk behaviour is not differentiated between outcome- and probability-ambiguous lotteries.

This phenomenon can be interpreted as a pessimistic expectation of the professionals, which amplifies their risk aversion and thus, makes them invest more when facing ambiguity. In a sense, professionals perceive the underlying probability distribution of mean-preserving spreads, as skewed. In real world risk assessment, it is most likely that probabilities of threats are expressed as ranges. This biased perception towards worst-case outcomes can be unnecessarily costly in information security investment, in case risk assessment follows similar quantitative methodologies.

In order to minimise subjectivity in ambiguity aversion, the underlying, and unknown, distributions of threat probabilities have to be approached as if they were normal. Using the expected values/losses as a point of reference can provide security professionals with a measure of comparison against their subjective expectations.

Historical Data on Past Security Events

All three interviewees (Section 5.4) agree that risk management should rely more on data and less on intuition. However, the amount of available data can vary significantly. In the case of ambiguity, historical data on past security events that provide ranges of probabilities and/or losses can be specified, and ambiguity aversion, if recognised, can be constrained. However, the provision of data cannot circumvent the inherent behavioural traits of the aforementioned risk and ambiguity aversion patterns. In other words, one of the points of this research is that even if organisations were to possess an exhaustive list of all threats along with their unambiguously associated probabilities of manifestation, this dataset would not ensure rational decision-making by security professionals. Needless to say, such complete datasets are exceedingly rare in practice.

5.5.2 Performance of Professionals and Students

Another question of potential interest is: how well do professionals perform in optimising decisions compared to the general population? In order to approach this question we perform comparisons between risk behaviour of information security professionals and the behaviour of a student sample. What is shown by the research findings is that both professionals and students deviate from expected losses minimisation and that they are both susceptible to choice inconsistencies and framing effects. Choice inconsistencies are identified by asking professionals about their WTP in order to avoid certain unfavourable lotteries and later, after other experiment tasks were completed, we asked them to chose between pairs of these same lotteries. Results are summarised

5.5 Discussion on Implications

in Table 3.5, in which professionals are found to be no more consistent than the student sample. In some cases, professionals also demonstrate higher ambiguity aversion than students (Figure 3.8). However, a possible familiarity of professionals with calculations of expected values and probabilities is reflected in Table 3.3, in which professionals, albeit not risk-neutral, state a WTP in order to avoid lotteries that is in almost all cases closer to the expected value of the lotteries than students' WTP. One interpretation of this is that professionals' ability to assess risks and minimise the consequence of threats has been shaped by the constant exposure to risk inherent to the security environment.

However, students are found to be more consistent with regards to perception of probabilities. Under the assumptions of salience theory, distortion of probabilities is found to be fairly consistent in the student sample, with the distortion being reasonably close to the objective probabilities. In contrast, professionals' choices are not consistent enough to allow for approximating the level of probability distortion. So, professionals exhibit susceptibility to framing effects, namely, to the presentation of risky choices, and this is very likely to imply a biased perception of probabilities.

So, quantitatively, we detect a proximity with expected values in professionals' WTP, but overall there is no qualitative difference in choice inconsistencies and deviations from expected values between students and professionals. Of course, professionals use their expertise and knowledge in evaluating information security requirements, prioritising measures and selecting mechanisms. But this expertise is not reflected in the maximisation of expected values, nor is demonstrated in the way they perceive probabilities, despite professionals' reported beliefs. From this perspective, expertise of security professionals does not provide an advantage in optimising investment levels.

5.5.3 Professional Roles

A number of role-dependent preferences of information security professionals are recorded. Namely, professionals report differences between prioritisation of decision criteria as a hypothetical question and as a role-based choice (Figures 5.12 and 5.12). As shown in Table 5.1 in the survey analysis of Section 5.3, seven out of the eleven criteria presented to professionals are self-reported with significantly different prioritisation, within-subjects. In particular the following criteria: estimation of expected losses, specification of exact threat probabilities, prioritising security, prioritising operational time, investment in large-probability threats, risk elimination and buying insurance are reported with different prioritisation from a hypothetical and a job role point of view.

Security and Operability

Preferences between security and operability are elicited in greater detail. Findings

5.5 Discussion on Implications

show that senior executives and compliance, risk, or privacy-related professionals are more security focused and that managerial roles prioritise operational time of tasks; IT-related professionals are split amongst priorities (Table 3.6). An explanation of the preference that senior executives exhibit for security might be that risk ownership, liability and a greater examination of the “big picture” of the security environment are closely associated with senior positions. Hierarchical superiors have a more clear view of the organisation’s needs and threats. Consequently, individuals in these positions might realise that a breach can turn out to be catastrophic, halting business processes. Thus, they choose the “safer path” of security prioritisation.

Both types of professionals, based on this dichotomous categorisation, exhibit loss aversion in their preferred attributes: they value the reduction of security/operability level in absolute terms twice as much as they value security/operability enhancement (loss aversion). So, professionals, depending on their role, tend to fear reduction of their prioritised attribute more than they would welcome enhancement of the same attribute.

The possibility of operability-focused professionals revealing more linear preferences between reduction/enhancement of security/operational time is also worth considering in decision-making, as it reveals more “balanced” preferences. In other words, operations-oriented professionals could be considered more objective or more practical with an approach that is more symmetrical between reduction and enhancement of the two attributes. This could imply that operations-related positions allow for a more balanced view of how security “fits” in the organisation.

So, professionals reveal different preferences in prioritising and evaluating the relative importance of security and operability, based on their professional roles. It would thus be misleading to assume that decision-makers approach risk-related issues independently of their position. Appreciation of this fact can be useful in achieving security investment agreements between involved parties from different parts of the organisation.

5.5.4 Proactive vs Reactive Security

Professionals reveal a preference for reducing losses compared to reducing the probabilities associated with these losses; this preference is manifested in hypothetical threat scenarios, i.e. in an information security context. All three interviewees welcomed this finding (Table 4.4). In particular, David Brewer stated that this is the way risk decisions should be thought of, i.e. as a means to minimise unwanted *consequences*. Paul Dorey highlighted that this is the training that professionals have, a focus on negative *impact* reduction, and Bruce Schneier suggested that this preference might indicate a choice for resilience over defence. The aforementioned explanation by which professionals consider low-impact losses inevitable, reinforces this finding. If small losses cannot

5.5 Discussion on Implications

be avoided, then the magnitude of the impact can be at least contained.

In addition, the possibility of eliminating risk completely is shown to be considered of secondary importance in our final survey (Figures 5.11 and 5.12). This finding can be considered to be in alignment with the experiment finding in which the possibility of eliminating risk completely does not increase professionals' WTP, so that professionals prefer to pay for reducing risk instead of eliminating it. As depicted in the ranks of Figures 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6, WTP for eliminating risk is significantly smaller than for reducing risk. Theory expectation is that risk elimination by paying, i.e. insurance buying, should be valued more by professionals as it creates a "certainty effect" on their perception and it also provides them with "a problem less to deal with". In this particular case, findings are differentiated from both expected loss minimisation and prospect theory. The most obvious explanation for this phenomenon is the realisation by security professionals that risk cannot be eliminated completely. This explanation was phrased by Bruce Schneier as "the futility of prevention" in Section 5.4.3 and it indicates that professionals are fully aware of the limitations of security measures, thus they exhibit a more realistic stance against potential threats. Thus, since perfect security is unreachable, professionals are inclined to contain damages after they occur.

Combining the aforementioned findings i.e. a preference for loss reduction and the absence of the risk-eliminating effect might signal professionals' realisation for the limitations of preventive security measures, and indicate a focus on resilience. These traits might explain a favourable stance towards reactive security programs.

It is important that decisions which balance preventive, detective and reactive security controls are clearly based on the impact analysis of potential threats on the business and on the assessment of risk, and that they are not vaguely implied in investment decisions. Thus, designing an overall investment plan based on the organisation's security strategy can provide a means to constrain certain behavioural traits of professionals which potentially violate maximisation of expected gains.

5.5.5 Framing

One of the most interesting research results, which has already been highlighted with relation to the student sample, is the susceptibility of professionals to framing effects. These are expressed by choice inconsistencies and dependency on the presentation of risky choices. We presented professionals with the same problems, but in different forms. Initially they had to pay in order to avoid a number of lotteries, and at a different stage of the experiment, they were asked to compare these same lotteries they were previously asked to avoid. Their choices between the two tasks are found to be inconsistent (Table 3.5).

5.5 Discussion on Implications

In the second experiment, we divided professionals into three random groups in which the same lotteries were presented as gains, losses, or “step-by-step” losses (Section 4.2.3.3). The three conditions were intended to simulate different budget allocations and perception of security investment as a necessary cost or as business enabling function. Elimination of risk is perceived as significantly different in the three condition groups (Figures 4.10, 4.11 and 4.12). In this sense, although a “budget frame” does not seem to influence attitude towards risk reduction, it has a significant effect on risk-elimination attitude.

If we were to hypothetically extend the conclusions of these findings, these would be of interest to risk management in organisations for a number of reasons. First, the way that budget is allocated can influence risk attitude of professionals; in our experimental setting findings indicate that they become more risk-averse if they have to consider budgets in a per-project allocation, rather than as investment extracted from a single budget. A possible explanation is that frequent budget allocation attracts the attention of professionals more, in contrast to a single initial allocation. Findings indicate that such a setting would cause professionals to invest more in insurance. Secondly, perceiving security investment as a business return function can make decision-makers more risk-averse than perceiving security as a necessary cost with no related return on investment. Notably, this view becomes more and more popular in the industry; due to the increasing reliance on IT systems, a lot of corporations push information security up in their agendas and, consequently, security is being perceived as an integral part of the business. Lastly, decision-makers underestimate the probabilities of almost certain gains more than they overestimate unlikely security losses. The fear for the prospect of not earning (business) gains is bigger than the fear of a rare security event manifesting.

It is notable that framing options can have an effect in two ways. On the one hand, e.g. perception of information security as a benefit or as a necessary cost can be part of the organisation culture and therefore might have an effect on security professionals when they examine investing in security controls. On the other hand, security professionals can present their proposed solutions to senior management, say, as return on investment mechanisms, and thus try to shift their risk perception accordingly.

5.5.6 Perception

Risk attitude in Professional Role and in Life

As far as perception of professionals is concerned, we observe in survey findings (Figure 5.3) that professionals consider that only 35.49% of other security professionals are willing to take risks. In their job role, the majority of professionals (52.26%) consider themselves as strictly risk taking, i.e. excluding risk neutrality, and 34.19% of them

5.5 Discussion on Implications

believe that they are more risk seeking than their colleagues. Risk seeking behaviour is more prevalent outside the professional context, so that 59.36% of professionals state that they are willing to take risks “in general”. More specifically, only 21.43% of professionals are willing to take more risks in their professional role than in their personal life. At the same time, survey findings report that only 24.52% of professionals consider themselves as risk-averse in general (Figure 5.4) and only 27.75% state that they are cautious and not willing to take risks in their professional roles (Figure 5.5).

So, the majority of professionals place themselves in the “risk-taking group” and they believe that the majority of other professionals are more risk-averse than them. In addition, these findings indicate that professionals are more cautious and less willing to gamble in the context of their professional roles in comparison to their general, risk behaviour in life.

Self-reported Risk Attitude and Experiment Findings

A related inconsistency is reported in our first survey (see Section 3.3.5), in which, remarkably, risk behaviour of professionals in some WTP tasks is found to be positively correlated with their own replies to the question: “How willing are you to take risks in general?” (see Table 3.7). So that professionals who report themselves as risk seeking reveal risk aversive behaviour in the experiment, and vice versa. Such an inconsistency is not observed in the student sample.

So, we observe that there are indications of distorted perception and self-perception of risk attitude amongst professionals. This fact can constitute a hindering factor in reaching security investment agreements in organisations. The reason is that if security professionals perceive risk differently than they act upon risk, they also possibly communicate risk the way they perceive it. Thus, justifying investment on quantitative arguments can be a way of minimising the risk-perception factor.

As highlighted in Section 2.1.2.1, it is an ISO 27000 recommendation that “perception of risk by affected parties should be taken into account” [81]. The aforementioned results indicate that such a goal may be hard-to-achieve.

Perception and Mathematical Skills

Professionals are found to deviate less from expected values than the student sample when they state their WTP to avoid lotteries, for both risk-averse and risk-seeking attitude. However, inconsistencies between choice and WTP are equally detected in both samples. Professionals are in some cases more ambiguity averse than students.

Despite the fact that only 5.17% of professionals consider themselves worse than the general population in their mathematical abilities and as many as 66.45% of them

5.5 Discussion on Implications

consider themselves better than the average person in terms of their mathematical skills in probabilities and expected values, professionals seem to deviate from maximisation of expected value about as often as the student sample (Figure 5.8).

So, overall, there is no qualitative difference between the performance of professionals and students in expected value maximisation, even if professionals self-report strong confidence in their mathematical skills. It would be to the benefit of professionals to appreciate the fact that their choices can be subjective and susceptible to biases.

5.5.7 Communication

Communication is a crucial factor in information security, because almost all decisions are ultimately made through a “propose, discuss, justify and accept” type of process. Paul Dorey (Section 5.4.2) insisted on the importance of aligned prioritisation between security professionals and business people, which is often absent in organisations. As elicited in the experiment of Section 3.6, professionals of different roles have significantly different preferences towards operational time and security measures. So, perception in information security depends on the position of the decision-maker, i.e. on the decision-maker’s job role point of view. This might be an understandable and maybe desirable attribute. However, a survey question on the perceived relative importance of security versus operational time from the perspective of the various professional roles, reveals a clear stereotypical and dichotomous perception that professionals have for the priorities of their colleagues. So, professionals have a biased view about what individuals consider important in each security role.

Such an inconsistency could imply that perception of information security from the perspective of various security roles is not communicated amongst professionals, or at least that professionals have their own stereotypical beliefs. We observe in Figure 5.9 that 118 out of 155 professionals believe that IT security related positions focus on security; and 125 out of the 155 professionals think that compliance, risk and privacy related people consider security as more important than operational time. At the same time, only 38 professionals indicate that security is more important for senior executives, and even less, namely 33 professionals, would indicate the same for managers. These numbers are almost symmetrically reversed in Figure 5.10, in which case senior executives and managers are believed to consider operational time as more important than security and vice versa for IT- and compliance-related professionals.

Prioritisation, perception and communication were discussed during our interviews. Paul Dorey mentioned that situations in which, for example, IT professionals are called to protect systems and processes without really knowing which of these assets constitute a priority for the organisation, are very common. David Brewer (Section 5.4.1) also

5.5 Discussion on Implications

pointed out the need for security professionals to communicate their message in a story-like scenario to their business counterparts, so that security investment suggestions can be evaluated in a common context.

Based on the observed differences in preferences and perception, we can safely state that priorities and objectives of the involved parties need to be shared for achieving more effective investment in information security.

5.5.8 De-biasing Decisions

Perhaps the most important message of this research is gaining a better understanding about how to de-bias the decision-making process. Such a goal cannot necessarily be achieved with explicit procedures and policies, but might be of a more elaborate nature. As was pointed out during the interviews, just pondering on the observed biases can be a first step in the objectification of decisions. For example, involved parties in the decision-making process could be made aware of the choice inconsistencies that professionals reveal (Section 3.3) or their significantly diversified risk attitude across framing scenarios (Section 4.3.3). Role-dependent preferences, budget allocation, the view of information security as a necessary cost or as a business enabler, risk aversion, ambiguity aversion, perception of risk, self-perceived risk attitude, preferences on risk treatment actions and prioritisation of decision-criteria, are all potential sources of subjectivity and biases in information security decision-making. Involved parties need to be aware that, for example, job positions shape prioritisation and influence perception of risk. It is not necessary that a risk owner has the most objective perception of a risk. Appreciation of the subjectivity of view can be a path to smoothing and normalising the effects of biases in the risk management processes.

Awareness of the involved parties is highly related with the importance of communication between, for example, business executives and security professionals, which has already been highlighted as a recommendation. Techniques for enhancing such communication are context- and structure-dependent and should be a goal for organisations.

Risk and ambiguity aversion, and in some cases risk taking behaviour, inevitably lead to over or underspending in security investment. Independently of the underlying sources of this behaviour, risk neutrality, with respect to expected losses, can serve decision-makers as a point of reference. Thus, unnecessary spending or pointless risk taking can be minimised.

Abstraction in Decision-making

Another need expressed by all interviewees is the objectification of decision-making via

5.5 Discussion on Implications

the use of data on previous security breaches, whenever possible. Making decisions on “abstracted” data can allow for the maximisation of expected value. Findings indicate the usefulness of abstraction as a means of de-biasing. For example, it might be practical to consider the option of buying insurance in an abstract way, other things being equal, when weighting expected benefits against the option of taking security measures on an asset. The reason is that these options are potentially related to subjective agendas and views. As, for example, in the case in which professionals prefer to take matters “into their own hands” by reducing risk, instead of transferring the risk to another party, e.g. by buying insurance.

However, this research indicates that the abstraction process is not a panacea. For example, preference of professionals for reduction of losses instead of probability reduction is only manifested in security scenarios and not in abstract lotteries. This implies that professionals take the security context into consideration. Namely, they possibly consider the futility of perfect security and the importance of reactive security and business continuity. In this sense, professionals take more factors into consideration than the abstracted version of the problem provides. Thus, we believe that implementation and context are inseparable parts of risk management and, consequently, abstraction can be effective only up to a certain level.

5.5.9 Discussion on Recommendations

Research findings on professionals’ risk perception and interviews with security experts suggest that the initial step for containing variability of bias-originated decisions is for the decision-makers to become self-aware of their susceptibility to biases in the first place. The recommendation of the ISO 27001 standard that “risk perception and risk attitude of involved parties, should be taken into consideration” can be transformed into a tangible precaution if the irrationality of the involved parties is, at least, recognised and accepted as a fact. Ensuring awareness amongst information security professionals and people from the business part of organisations regarding potentially “irrational” decisions and biases is a first step for de-biasing investment decisions.

Decision-makers can minimise unnecessary spending or avoid the insecurity of under-spending if they use maximisation of expected profits as a measure for evaluating risk-related investment choices. That is, professionals’ experimentally elicited systematic risk-averse and risk-seeking behaviour across a variety of risky and ambiguous circumstances, can be constrained.

It is highlighted in this research that there are significant differences between the various roles of professionals regarding risk perception, ranking of security controls, prioritisation of system attributes, even misaligned perception about the risk behaviour of other

5.5 Discussion on Implications

professionals. In that sense, the role-dependent perception of professionals in combination with insufficient communication during the decision-making process can lead to a misalignment of priorities and dissonance on how to manage risk. Decision-makers and managers need to be able to identify these asymmetries in perception in order to be able to agree on optimal investment levels.

With the exception of a few cost-independent decisions, like e.g. regulatory and legal requirements, all information security investment decisions are ultimately made with costs and benefits in mind. Such decisions require a direct communication between people inside the business and professionals who are closely involved with information security. In order for this relation to be constructive, both parties need to speak the “same language” and operate on the same decision context. Thus, a crucial point in information security is how threats, impact and risk are conveyed to senior and business management by security professionals.

The aforementioned research findings indicate the need for a close and factual communication, that is based on available data, whenever possible, for bridging the gaps regarding incentives and perspectives of the involved parties. This communication needs to be aligned with the business objectives and the information security needs of the organisation. In order to overcome the diversity of risk perception and the out-of-balance prioritisation, discussions need to be based, as much as possible, on quantitative factual evidence.

Framing decisions in different ways can shift behaviour significantly, including how professionals perceive risk or how they present security solutions to senior management. For example, findings indicate that viewing information security as a positive contributor to the business can increase decision-makers’ risk aversion. This means that an organisation that views security as a business enabling function, might be willing to invest more in security. In contrast, security as a necessary cost can hinder willingness to invest.

Security problems, if examined in isolation, might lead to different decisions due to framing effects. Research results on framing effects should concern any decision maker who would like to believe that the security recommendations they propose do not depend on the way in which questions were asked. Even widespread frameworks, like the ISO series of standards, encourage customised approaches for risk assessments based on the needs of each organisation. Moreover, a universal approach to risk management is not expected to be seen in the near future. These two factors suggest that context dependency and diversification of investment decisions due to framing effects can be seen as norm and not as an exception in information security. Providing a descriptive pluralism for examining these problems under the perspective of various framing options can minimise these effects. This fact could also mean that targeted interventions in

5.5 Discussion on Implications

risk presentation and risk communication policies can “nudge” decisions in information security investment towards desirable directions.

In order to restrict the margins that allow for inherent behavioural traits of decision-makers to be manifested, organisations can define and communicate their business objectives, and subsequently their information security goals. Such an approach can be realised as a practical and understandable information security strategy, communicated as a policy across the organisation. In this context, if investment-related variables are identified and hidden factors left to the decision-makers’ judgement are limited, abstracting security investment decisions in a quantitative fashion can further strengthen the security posture and thus, the benefit of the organisation.

5.5.10 Summary

In this Chapter we focused on the most important experimental results and we presented a supplementary survey for further exploring risk perception of information security professionals. We discussed potential implications of the research with renowned security experts and we provided recommendations for minimising the observed behavioural biases.

Survey results indicated that prioritisation of decision criteria depends on the professionals’ role. Professionals were found to consider themselves as being risk-seeking in general, and more risk-seeking than their colleagues. They also consider other security professionals as being overall risk-averse. The majority of professionals reported that their mathematical skills are better than the average person’s. Stereotypical perceptions regarding security roles and prioritisation between security and operability were also traced.

Interviews with security experts highlighted the importance of risk perception and attitude in information security, and the significance of behavioural research in the field. Interviewees pointed out the need for clear communication of risk amongst involved parties and the need to de-bias decision-making by basing it on factual data, avoiding individual judgement.

We categorised and discussed implications of the research findings, providing an interpretation of the findings’ consequences in real-world environments. Finally, we recommended a number of actions that can be taken by organisations, in order to optimise information security investment decisions and to minimise risk-related biases of the decision-makers.

Conclusion

Information security is a field with inherent risk and uncertainty. Organisations and policy makers have sought to reduce the impact of these issues; for example, by gathering data on past security breaches or passing new disclosure laws which increase public knowledge about the distribution of breaches. Despite these efforts to collect information, the complexity and uniqueness of information security systems often only allow organisations to approximate ranges of probabilities and of damages associated with potential threats and vulnerabilities. Thus, risk management and security investment are, by nature, characterised by ambiguity and uncertainty. This research examined how information security professionals make decisions in such an environment and, specifically, whether security professionals are rational decision-makers who minimise expected losses.

In our exploration of decision-making in information security investment, we focused on the individual risk behavioural traits which active professionals and practitioners exhibit. In a field in which standardisation and best practises flourish, one would expect that the correctness of information security decisions might be objectively justifiable. It becomes apparent from the experimental findings that risk attitude, and consequently investment decisions, are influenced by inherent behavioural traits and by the approach of risk management taken by an organisation.

Under expected utility theory, which is the standard normative decision-making approach, a rational decision maker should minimise expected losses or maximise expected gains. However, behavioural economics has repeatedly demonstrated that most individuals systematically deviate from expected utility maximisation. We examined three well-known behavioural anomalies: risk and ambiguity aversion, worst-case aversion, and other-evaluation. We also examined an additional two industry-specific types of behaviour, namely a preference for security over operability and a variety of preferences related to risk treatment actions. We examined these behaviours using experiments and surveys which elicit preferences using simple, neutrally-framed lotteries as well as scenario-specific lotteries. We compared decision-making of professionals to a sample of university students.

6.1 Key Research Findings

We conclude the thesis by presenting the key research findings and possible future research.

6.1 Key Research Findings

Across a variety of lotteries, information security professionals consistently indicated a willingness to pay to avoid negative outcomes that was closer to the expected losses than did the sample of students.

Despite their greater ability to assess risk, our findings suggest that security professionals still have distinctive behavioural characteristics which deviate from expected utility theory. In common with the student sample, and with a number of other studies, the observed behaviour of professionals follows the pattern of risk attitudes described by Kahneman and Tversky [90]. Security professionals exhibit significant risk aversion when faced with low possibilities of loss or small losses. However, their actions switched from being risk-averse to being risk-seeking when faced with large probabilities of losses or large losses. In a similar finding, based on the predictions of salience theory, professionals exhibit a highly distorted perception of probabilities.

Information security professionals also show considerable ambiguity aversion in the experiments. Their willingness to pay increased significantly, compared to risky lotteries, when faced with low- and moderate-probability lotteries which had ambiguous probabilities and/or outcomes. As with risk, ambiguity is an inherent feature of the information security environment, which is characterised by unknown or imperfectly known threats.

Additionally, a significant number of professionals display preference reversal depending on whether a decision is framed as a choice or as WTP, similarly to the student sample.

Framing risk decisions as losses, gains or individually separated losses is also shown to diversify risk attitude of professionals significantly. Professionals are more risk-averse when confronted by gains-related decisions than when they deal with losses. They are also more risk-averse when potential losses are subtracted from individual budgets in comparison to when losses apply on a single budget, with regards to risk transfer.

Professionals are willing to pay more than the expected value of lotteries in order to reduce probabilities and losses of these lotteries comparatively to paying for securing a zero loss. Thus, professionals reveal a preference for paying to *modify* risk rather than paying to *eliminate* risk completely, which is the equivalent of *risk transfer* in risk management terminology.

6.2 Future Research

When presented with information security threat scenarios professionals reveal an inclination for reducing losses instead of minimising the probabilities that generated these losses. So, professionals have distinct preferences for treating risk, even if the expected value of the alternatives is the same.

Finally, we examined security professionals' preferences between operability and security. Preferences across individuals are heterogeneous and we also find that preferences between security and operability are correlated with professional role.

Survey findings indicate biased, stereotypical expectations amongst professionals regarding the priorities that professionals in other positions exhibit. Prioritisation of a variety of decision criteria in information security measures is also found to be diversified across security positions. In our surveys, the majority of professionals report themselves as being more risk seeking than their colleagues. These findings reveal the existence of biased perceptions and misaligned prioritisation in the security work environment.

Taking this evidence as a whole, we would not characterise security professionals as fully rational decision-makers. This implies that calculations involved in risk assessment methodologies and perceptions of risk are dependent on the decision-maker's subjective perceptions. This is potentially an aspect of risk management and decision-making in information security investment that needs to be strengthened.

6.2 Future Research

There are several research questions that emerge from this study and could be further examined. For example, the extent to which ambiguity aversion is probability- or outcome-dependent was outside the scope of our study, so more research could shed light into this area. Also, we did not examine which type of problem-framing (WTP or choice) tends to lead to better decisions (i.e. closer to expected value maximisation), so more research might be needed on framing effects in information security.

The effect that the culture of an organisation can have on risk perception and security awareness could also be explored further. Good information security practice can only be achieved by a combination of security-aware professionals, management and employees. Having people involved in security processes shapes their stance towards risk. Threats should also be communicated appropriately in order to achieve the desired level of employee-commitment.

Having established the existence of professionals' biases related to risk perception and risk attitude, it is worth considering the potential effects of the actual security envi-

6.2 Future Research

ronment. For this reason, we plan to target our future research on the examination of risk behaviour in real-world security contexts. For example, in situations of pressure and urgency people might “bend the rules” to complete daily tasks. As a result, security procedures are often bypassed for the sake of “getting the job done”. Such an attitude inevitably creates more risk. The types of security controls, including technical, operational or administrative controls, which can assist in making security policies acceptable, and thus enforceable, are yet to be examined.

At a different level, the relationship between management and security professionals could be further studied in the specific context and structure of organisations. It is the senior management and business parts of the organisation that take actions for treating risk. However, thresholds of risk acceptability can be flexible and risk can be underweighted due to a narrow focus on business operations only. Specifying which types of risk communication methods between security and business professionals can be deployed in order to base decisions on concrete variables, would be of great value.

Some further behavioural patterns might be interesting to explore. The “follow the crowd” behaviour of security professionals, by which security programs adopt trending technologies due to peer benchmarking, has already been mentioned. Such a phenomenon potentially affects the security industry as a whole, since it maintains or re-enforces trends in products and practices at the expense of other possibly more optimal solutions. Gaining insight into the processes and motivations that cause this or similar behaviours would be highly beneficial for managing information security risk.

Finally, risk management approaches can be investigated through the prism of various industries, by taking into consideration the characteristics of each sector. Designing industry-specific methodologies for assessing and treating risk might provide organisations with more flexible tools for enhancing the process of managing risk.

Appendices

A.1 Appendix: Experiment 1

A.1.1 Experiment Design

A.1.2 H1 Instrument

There are four types of experiment questions on willingness to pay to avoid a lottery, one for each lottery type. The actual values of p_i and x_i are shown in the second and third column of Table A.1:

“What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is a $p\%$ probability of losing \$50 and losing nothing otherwise?”.

“What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is a probability between $p_1\%$ and $p_2\%$ of losing \$50?”.

“What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is a $p\%$ probability of losing an amount between $\$x_1$ and $\$x_2$ and losing nothing otherwise?”.

“What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is a probability between $p_1\%$ and p_2 of losing an amount between $\$x_1$ and $\$x_2$ and losing nothing otherwise?”.

A.1 Appendix: Experiment 1

Table A.1: H1 Instrument

#	Prob. ($p\%$)	Outcomes (x in \$)	WTP	EV μ	Exp. Outcome Interval	Outcome Range
H_{11}	5	-50	0 to 100	-2.5	-2.5	0
H_{12}	0-10	-50	0 to 100	-2.5	[-5, 0]	5
H_{13}	5	-80 to -20	0 to 100	-2.5	[-4, -1]	3
H_{14}	0-10	-80 to -20	0 to 100	-2.5	[-8, 0]	8
H_{15}	15	-50	0 to 100	-7.5	-7.5	0
H_{16}	0-30	-50	0 to 100	-7.5	[-7.5, 0]	7.5
H_{17}	15	-80 to -20	0 to 100	-7.5	[-12, -3]	9
H_{18}	0-30	-80 to -20	0 to 100	-7.5	[-24, 0]	18
H_{19}	50	-50	0 to 100	-25	-25	0
H_{110}	35-65	-50	0 to 100	-25	[-32.5, -17.5]	15
H_{111}	50	-80 to -20	0 to 100	-25	[-40, -10]	30
H_{112}	35-65	-80 to -20	0 to 100	-25	[-52, -7]	45

A.1.3 Lottery Comparisons

Hypothesis 2 Question 1 (H_{21})	
Lottery A (Lottery 9)	Lottery B (Lottery 10)
a probability of 85% of losing 45	a probability of 85% of losing 50
a probability of 8% of losing 220	a probability of 8% of losing 170
a probability of 3.5% of losing 300	a probability of 3.5% of losing 300
a probability of 2.5% of losing 450	a probability of 2.5% of losing 400
a probability of 1% of losing 900	a probability of 1% of losing 1000
$\mu = -86.6, Var = 14406.2$	$\mu = -86.6, Var = 14087.4$

Hypothesis 2 Question 2 (H_{22})	
Lottery A (Lottery 10)	Lottery B (Lottery 11)
a probability of 85% of losing 50	a probability of 85% of losing 45
a probability of 8% of losing 170	a probability of 8% of losing 250
a probability of 3.5% of losing 300	a probability of 3.5% of losing 350
a probability of 2.5% of losing 400	a probability of 2.5% of losing 450
a probability of 1% of losing 1000	a probability of 1% of losing 800
$\mu = -86.6, Var = 14087.4$	$\mu = -89.75, Var = 14416.2$

Hypothesis 2 Question 3 (H_{23})	
Lottery A (Lottery 8)	Lottery B (Lottery 6)
a probability of 15% of losing nothing	a probability of 15% of losing nothing
a probability of 30% of losing 200	a probability of 30% of losing 166.66
a probability of 30% of losing 300	a probability of 30% of losing 300
a probability of 20% of losing 450	a probability of 20% of losing 450
a probability of 5% of losing 700	a probability of 5% of losing 900
$\mu = -275, Var = 28375$	$\mu = -274.998, Var = 40708.8$

A.1 Appendix: Experiment 1

Hypothesis 2 Question 4 (H_{24})	
Lottery A (Lottery 6)	Lottery B (Lottery 7)
a probability of 15% of losing nothing	a probability of 15% of losing nothing
a probability of 30% of losing 166.66	a probability of 30% of losing 183.33
a probability of 30% of losing 300	a probability of 30% of losing 300
a probability of 20% of losing 450	a probability of 20% of losing 450
a probability of 5% of losing 900	a probability of 5% of losing 800
$\mu = -274.998$, Var = 40708.8	$\mu = -274.999$, Var = 33958.5

Hypothesis 2 Question 5 (H_{25})	
Lottery A (Lottery 4)	Lottery B (Lottery 12)
a probability of 85% of 50	a probability of 85% of 46
a probability of 8% of losing 150	a probability of 8% of losing 180
a probability of 3.5% of losing 300	a probability of 3.5% of losing 350
a probability of 2.5% of losing 450	a probability of 2.5% of losing 480
a probability of 1% of losing 1000	a probability of 1% of losing 900
$\mu = -86.25$, Var = 14698.4	$\mu = -86.75$, Var = 15012.5

A.1.4 H2 Willingness-to-pay Lotteries

Hypothesis 2 Question 6 (H_{26})
Lottery 9: How much are you willing to pay in order to avoid playing a lottery in which there is:
a probability of 85% of losing 45
a probability of 8% of losing 220
a probability of 3.5% of losing 300
a probability of 2.5% of losing 450
a probability of 1% of losing 900
$\mu = -86.6$, Var = 14406.2

Hypothesis 2 Question 7 (H_{27})
Lottery 10: How much are you willing to pay in order to avoid playing a lottery in which there is:
a probability of 85% of losing 50
a probability of 8% of losing 170
a probability of 3.5% of losing 300
a probability of 2.5% of losing 400
a probability of 1% of losing 1000
$\mu = -86.6$, Var = 14087.2

Hypothesis 2 Question 8 (H_{28})
Lottery 11: How much are you willing to pay in order to avoid playing a lottery in which there is:
a probability of 85% of losing 45
a probability of 8% of losing 250
a probability of 3.5% of losing 350
a probability of 2.5% of losing 450
a probability of 1% of losing 800
$\mu = -89.75$, Var = 14416.2

A.1 Appendix: Experiment 1

A.1.4.1 Consent Form

Experiment 1: Consent Form

Thank you for taking part in this experiment and survey! Your participation is very helpful for my cross-disciplinary PhD research in the Information Security Group and Economics Department at Royal Holloway University of London!

Konstantinos

Procedure:

You will be asked to complete a number of short lottery-type experiments and a survey with Information Security related questions and demographics. Duration is no more than about 15 minutes.

Benefits and Scope of this Study:

First of all, your participation will allow me to collect valuable data for my PhD research! By completing all questions you earn a symbolic participation fee of \$3. Additionally, you are given an amount of \$10 to ‘play’ in the lotteries. After completing the survey, one of the lotteries will be randomly selected and played for you. All lotteries are over losses and the resulting loss will be proportionally reduced from your \$10 and the remainder will be your additional payment. So, your potential maximum payment is \$13. An email will be sent to your designated email address with your payment in the form of an Amazon gift certificate. Please, note that for the payment to be processed all answers will be validated to avoid ‘random’ replies.

Confidentiality:

No identification of the participants is collected or maintained during or after the completion of the experiments and the survey and all data are fully anonymised. An email address is requested at the end of the survey only for the purpose of sending your payment. All data will be protected and kept completely confidential. No data hard copies will be kept at any point of the research.

Usage of the findings:

The research findings will be used for academic purposes only. For example, they might be presented in academic conferences, and be published in research journals in the field of Information Security and Economics. Research findings will be made available to all participants upon request after data collection and data analysis.

Contact information:

In case of any concern or question, please contact Konstantinos at konstantinos.mersinas.2011@live.rhul.ac.uk or call directly at +44.. . By beginning the survey you acknowledge that you have read this form and agree to participate in this research.

A.1 Appendix: Experiment 1

A.1.5 Survey Questions

Question: “Are you related with the profession or practice of Information Security in any way?” *Yes / No*

Question: “How many years of experience do you have in Information Security related tasks?”

Question: “How willing are you to take risks in general?” *0 to 10*
0: Not willing at all 10: Very willing

Question: “Your job title most closely resembles:”

- *Senior executive role (e.g. CEO, CIO, CISO, CSO etc.)*
- *Managerial role (e.g. Project Manager, IT Director, Security Manager etc.)*
- *IT & Security (e.g. Security Officer, System Administrator, Cyber Security Information Analyst etc.)*
- *Compliance, Risk or Privacy role (e.g. Governance, Risk and Compliance Consultant, Information Security Consultant, Auditor etc.)*
- *Other: please specify*

Question: “Does your job position allow you to make independent Information Security related decisions?” *Yes / No*

Question: “How worried are you that a severe/important security incident might materialise in your company / organisation, despite the existing protective measures?” *0 to 10*
0: Not worried at all 10: Very worried

Question: “How worried are you about new unidentified information security threats?” *0 to 10*
0: Not worried at all 10: Very worried

A.1 Appendix: Experiment 1

Question: "Have you experienced any important security incident in the past?"
Yes / No

Question: "How closely related do you think investment in Information Security is to business objectives?" *0 to 10*
0: Not related at all 10: Very much related

Question: "How much do you think companies / organisations focus on business operations and as a result underestimate or neglect security?" *0 to 10*
0: Not worried at all 10: Very worried

Question: "Where / to whom does your Chief Information Security Officer (CISO or CSO) or equivalent senior executive report?"

Question: "What is the size of your company?"

Question: "What is your gender?"

Question: "What is your age?"

Question: "What is your educational level?"

Question: "What is your marital status?"

Question: "What is the number of dependents in your family?"

Question: "What is your approximate annual income in British pounds?"

Question: "Which country do you live in?"

A.1 Appendix: Experiment 1

Question: “What is your nationality?”

Question: “What is your mother tongue?”

A.1.6 Experiment 1 Indicative Screenshots

Figure A.1: The “other-evaluation and behaviour” hypothesis statement is randomly presented to half of the participants.

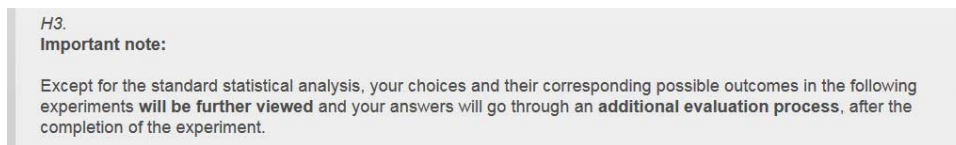
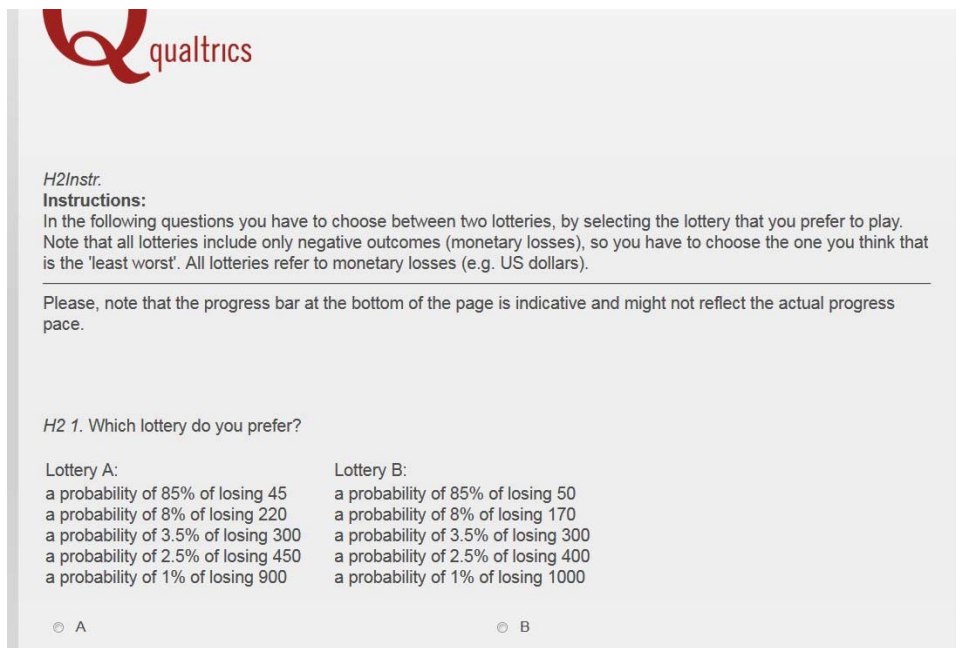


Figure A.2: The first task that is presented to participants involves five comparisons between lotteries. The first comparison is presented below.



A.1 Appendix: Experiment 1


Figure A.3: In the next task, participants are asked to state their willingness to pay in order to avoid three lotteries of the following form.

H2InstrWTP. Instructions:
Imagine that you have to play a lottery with only negative outcomes.
You can avoid playing the lottery if you pay an amount of money.

The following questions require you to specify the *maximum* amount that you are **willing to pay** so that you **will not have to participate** in the unfavourable lottery.

Note: you can *click and drag* the bar for specifying an exact value.

H2 6. What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is:
a probability of 85% of losing 45
a probability of 8% of losing 220
a probability of 3.5% of losing 300
a probability of 2.5% of losing 450
a probability of 1% of losing 900 ?



0 100 200 300 400 500 600 700 800 900

\$

Figure A.4: Relative importance between security and operations is tested by a series of questions with the following design.

H5 1Instr. Instructions:
In the following questions you can consider 'Security' as the level of protection of the system, and 'Operability' as the time needed to complete tasks.
In other words, you are asked to choose between protection and operational efficiency.

H5 1. Imagine the following scenario:

You are managing an Information System that has moderate-impact on the confidentiality, availability and integrity of information records kept by your organisation.
The total worth of the system under protection is evaluated at \$10,000.
Full operability of the system allows the business to gain a profit of \$10,000.

Two new mechanisms A and B with the same cost are proposed for the system.
Which one of the following mechanisms do you prefer?

	Mechanism A Enhances Security of the system by 10%	Mechanism B Enhances Operability of the system by 10%
I prefer:	<input type="radio"/>	<input type="radio"/>

Click to write Column 1

A.1 Appendix: Experiment 1

Figure A.5: Subsequent questions are dynamically formed by the choices of participants.

qualtrics

H5 1B-10.9. You are managing an Information System that has moderate-impact on the confidentiality, availability and integrity of information records kept by your organisation.
The total worth of the system under protection is evaluated at \$10,000.
Full operability of the system allows the business to gain a profit of \$10,000.

Two new mechanisms A and B with the same cost are proposed for the system.
Which one of the following mechanisms do you prefer?

	Mechanism A Enhances Security of the system by 10%	Mechanism B Enhances Operability of the system by 9%
I prefer:	<input type="radio"/>	<input type="radio"/>

>>

0% 100%

Figure A.6: Similarly to a previous section, the following questions elicit willingness to pay in order to avoid lotteries.

qualtrics

Q210. Instructions for the next section:
Similarly to the first section, imagine that you are taking part in a lottery with only negative outcomes. The best possible outcome of the lottery is a zero loss.
The amount that you might lose can be exact, say \$50, or uncertain, e.g. any amount between \$20 and \$80.
Also, the probability of losing can be exact, say 50%, or uncertain, e.g. any probability between 35% and 65%.

Again, the following questions require you to specify the **maximum** amount that you are **willing to pay** so that you **will not have to participate** in such an unfavourable lottery.

>>

0% 100%

A.1 Appendix: Experiment 1

Figure A.7: This screenshot shows an example of willingness to pay stated by a participant (presentation of this part is randomised between: risky lotteries being presented first and being followed by ambiguous lotteries, or vice versa).

H1 4ar. What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is a probability between 0% and 10% of losing an amount between \$20 and \$80 and losing nothing otherwise?

0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80

\$ 0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 **6**

H1 8ar. What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is a probability between 0% and 30% of losing an amount between \$20 and \$80 and losing nothing otherwise?

0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80


\$ 0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 **24**

H1 12ar. What is the maximum amount that you are willing to pay in order to avoid playing a lottery in which there is a probability between 35% and 65% of losing an amount between \$20 and \$80 and losing nothing otherwise?

0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80

\$ 0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 **57**

Figure A.8: The next section contains the mechanism for measuring relative loss aversion in either security or operations, based on previous choices of the participant.



H5 2B-10,8. You are managing an Information System that has moderate-impact on the confidentiality, availability and integrity of information records kept by your organisation.
The total worth of the system under protection is evaluated at \$10,000.
Full operability of the system allows the business to gain a profit of \$10,000.

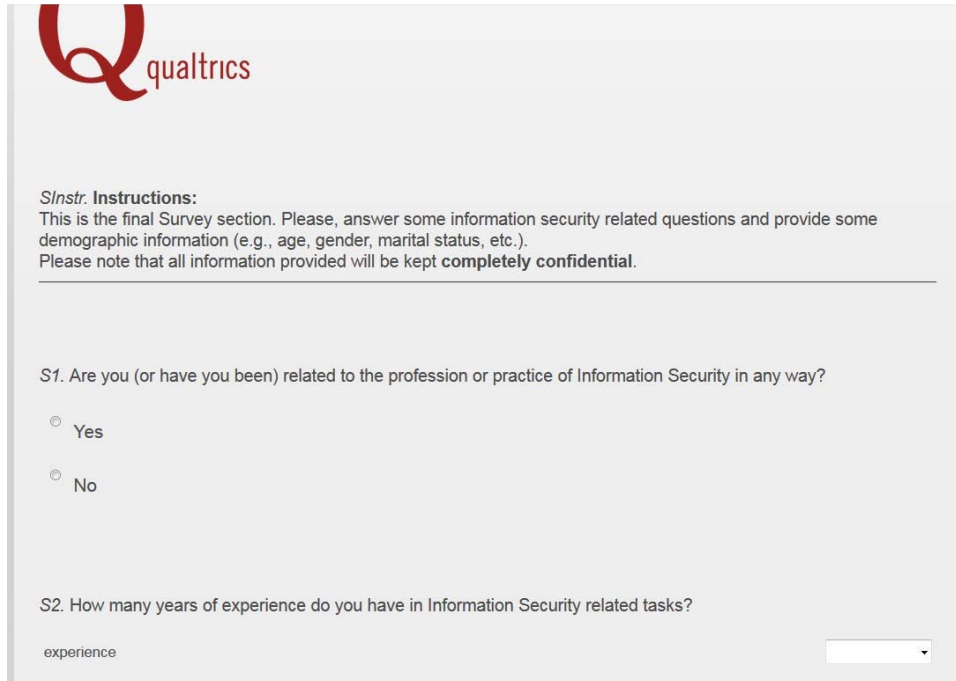
Would you prefer:
A: to remain in the current state of the system
B: to implement mechanism B (suppose that there is no additional cost for implementing mechanism B) or
C: A and B is the same to you?


	Choice A: Remain at the current system state	Mechanism B: Enhances Security by 10% Reduces Operability by 8%	Choice C: A and B are the same to me
I prefer:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

0% 100%

A.1 Appendix: Experiment 1

Figure A.9: The final section comprises the survey and demographic questions.





Instructions:
This is the final Survey section. Please, answer some information security related questions and provide some demographic information (e.g., age, gender, marital status, etc.).
Please note that all information provided will be kept **completely confidential**.

S1. Are you (or have you been) related to the profession or practice of Information Security in any way?

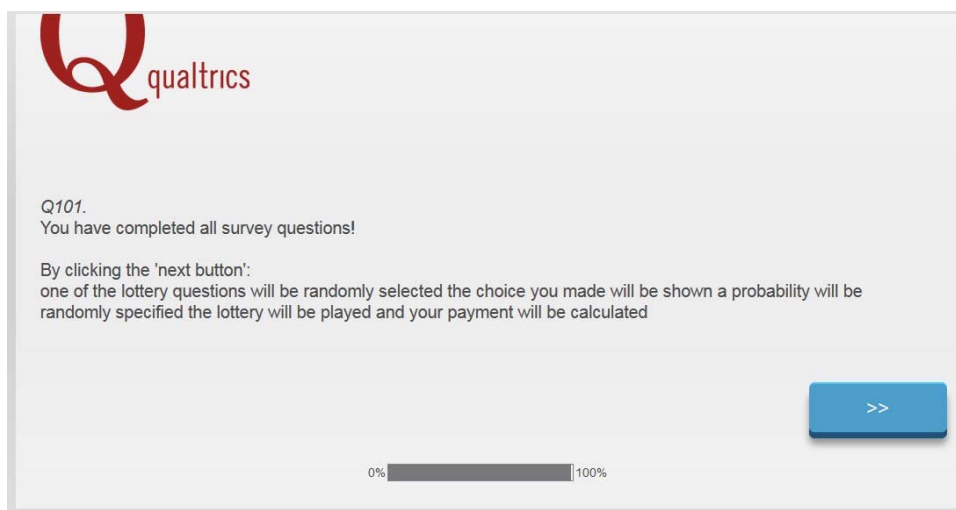
Yes


No

S2. How many years of experience do you have in Information Security related tasks?

experience

Figure A.10: Each participant is informed about the payment procedure.





Q101.
You have completed all survey questions!

By clicking the 'next button':
one of the lottery questions will be randomly selected the choice you made will be shown a probability will be randomly specified the lottery will be played and your payment will be calculated

0% 100%

A.1 Appendix: Experiment 1

Figure A.11: The final payment is presented to the participant.

Q102.
Your performance-based payment calculation:

Question No 20 was randomly chosen:
"Which lottery do you prefer?"


Lottery A: a probability of 15% of losing nothing a probability of 30% of losing 166.66 a probability of 30% of losing 300 a probability of 20% of losing 450 a probability of 5% of losing 900 "	Lottery B: a probability of 15% of losing nothing a probability of 30% of losing 183.33 a probability of 30% of losing 300 a probability of 20% of losing 450 a probability of 5% of losing 800 "
--	--

your answer to this question was: **B**

The probability that is randomly drawn for the lottery is: **0.478374655071956**
and the lottery outcome is: **300**

This outcome proportionally corresponds to: \$3.75 out of \$10.
By subtracting this loss from your initial amount of \$10, your additional payment is \$6.25 !
And your total payment (participation fee plus additional payment) is \$9.25.

Please, click the 'next button' to finalise the survey.



A.1 Appendix: Experiment 1

A.1.7 Qualtrics Javascript Code

```
1  Qualtrics.SurveyEngine.addOnload(function()
2  {
3  var maxpayment = 10;
4  var participationfee = 3;
5  var y2 = maxpayment;
6
7  function LinearMap(x, x1, x2, y1, y2)
8  {
9
10 var map = ((y2-y1)/(x2-x1))*(x-x1)+y1;
11 return Math.round(map*100)/100;
12 }
13
14 function DelayFunction()
15 {
16 setTimeout(load,3000); // 3000 milliseconds
17 return;
18 }
19
20 var n=27; //the number of entries in the Array
21
22 var AnswerPayment = new Array(n);
23 for (var i = 0; i < n; i++)
24 {
25 AnswerPayment[i] = new Array(5);
26 }
27 // each entry x has:
28 // in position [][0] the answer VALUE
29 // in position [][1] the corresponding additional PAYMENT for that Answer
30 // in position [][2] the question TEXT is stored
31 // in position [][3] the random OUTCOME of the lottery is stored
32 // in position [][4] the normalised LOSSES
33
34 //ASSIGNING ANSWERED VALUES TO AnswerPayment ARRAY, FOR HYPOTHESIS 1 (16 Slots
   : from 0 to 15)
35 //Alternative way: AnswerPayment[0][0] = "${q://QID2/ChoiceNumericEntryValue
   /1}";
36 AnswerPayment[0][0] = "${e://Field/H1Answer1}";
37 AnswerPayment[1][0] = "${e://Field/H1Answer2}";
38 AnswerPayment[2][0] = "${e://Field/H1Answer3}";
39 AnswerPayment[3][0] = "${e://Field/H1Answer4}";
40 AnswerPayment[4][0] = "${e://Field/H1Answer5}";
41 AnswerPayment[5][0] = "${e://Field/H1Answer6}";
42 AnswerPayment[6][0] = "${e://Field/H1Answer7}";
43 AnswerPayment[7][0] = "${e://Field/H1Answer8}";
44 AnswerPayment[8][0] = "${e://Field/H1Answer9}";
45 AnswerPayment[9][0] = "${e://Field/H1Answer10}";
46 AnswerPayment[10][0] = "${e://Field/H1Answer11}";
47 AnswerPayment[11][0] = "${e://Field/H1Answer12}";
48 AnswerPayment[12][0] = "${e://Field/H1Answer13}";
49 AnswerPayment[13][0] = "${e://Field/H1Answer14}";
50 AnswerPayment[14][0] = "${e://Field/H1Answer15}";
51 AnswerPayment[15][0] = "${e://Field/H1Answer16}";
52
```

A.1 Appendix: Experiment 1

```
53 //ASSIGNING PAYMENTS FOR HYPOTHESIS 1 //note: I store the OUTPUT losses as a
    POSITIVE number. Then I calculate: OUTCOME -
54
55 Investment(WTP) = LOSSES
56 //explanation of losses: if [][1] is NEGATIVE it means that the lottery outcome
    was 0 and the participant only has to pay his INVESTMENT
57
58 // if [][1] is POSITIVE it means that the lottery produced some LOSS and the
    participant actually MINIMISED the LOSS by his investment, so he only lost
    the positive amount instead of losing more
59
60 var num = Math.random();
61 var ambig0to10 = Math.random()*0.1;
62 var ambig0to30 = Math.random()*0.3;
63 var ambig35to65 = Math.random()*0.3+0.35;
64 var ambig75to100 = Math.random()*0.25+0.75;
65 var ambig20to80 = Math.floor((Math.random()*0.6)*100+20);
66
67 //document.write("num = ", num);
68 //document.write("<br>");
69 //document.write("ambig0to10 = ", ambig0to10);
70 //document.write("<br>");
71 //document.write("ambig0to30 = ", ambig0to30);
72 //document.write("<br>");
73 //document.write("ambig35to65 = ", ambig35to65);
74 //document.write("<br>");
75 //document.write("ambig75to100 = ", ambig75to100);
76 //document.write("<br>");
77 //document.write("ambig20to80 outcome = ", ambig20to80);
78 //document.write("<br>");
79 //document.write("<br>");
80
81 //Question H1 1
82 if (num <= 0.05) {AnswerPayment[0][3] = 2.5;} else {AnswerPayment[0][3] = 0;}
83 AnswerPayment[0][1] = AnswerPayment[0][3] - Number(AnswerPayment[0][0]); //
    outcome minus WTP
84 AnswerPayment[0][4] = LinearMap(AnswerPayment[0][1], 0, 50, 0, maxpayment);
85
86 //document.write("lottery 1 outcome is: ", AnswerPayment[0][3], " answer was ",
    AnswerPayment[0][0], " and your losses are: ",
87
88 AnswerPayment[0][1], " and the linear mapping is GBP", AnswerPayment[0][4]);
89 //document.write("<br>");
90
91 //Question H1 2
92 if (num <= ambig0to10) {AnswerPayment[1][3] = 50;} else {AnswerPayment[1][3] =
    0;}
93 AnswerPayment[1][1] = AnswerPayment[1][3] - Number(AnswerPayment[1][0]);
94 AnswerPayment[1][4] = LinearMap(AnswerPayment[1][1], 0, 50, 0, maxpayment);
95
96 //document.write("lottery 2 outcome is: ", AnswerPayment[1][3], " answer was ",
    AnswerPayment[1][0], " and your losses are: ",
97
98 AnswerPayment[1][1], " and the linear mapping is GBP", AnswerPayment[1][4]);
99 //document.write("<br>");
100
101 //Question H1 3
```


A.1 Appendix: Experiment 1

```
102 if (num <= 0.05) {AnswerPayment[2][3] = ambig20to80;} else {AnswerPayment[2][3]
    = 0;}
103 AnswerPayment[2][1] = AnswerPayment[2][3] - Number(AnswerPayment[2][0]);
104 AnswerPayment[2][4] = LinearMap(AnswerPayment[2][1], 0, 80, 0, maxpayment);
105
106 //document.write("lottery 3 outcome is: ", AnswerPayment[2][3], " answer was ",
    AnswerPayment[2][0], " and your losses are: ",
107
108 AnswerPayment[2][1], " and the linear mapping is GBP", AnswerPayment[2][4]);
109 //document.write("<br>");
110
111 //Question H1 4
112 if (num <= ambig0to10) {AnswerPayment[3][3] = ambig20to80;} else {AnswerPayment
    [3][3] = 0;}
113 AnswerPayment[3][1] = AnswerPayment[3][3] - Number(AnswerPayment[3][0]);
114 AnswerPayment[3][4] = LinearMap(AnswerPayment[3][1], 0, 80, 0, maxpayment);
115
116 //document.write("lottery 4 outcome is: ", AnswerPayment[3][3], " answer was ",
    AnswerPayment[3][0], " and your losses are: ",
117
118 AnswerPayment[3][1], " and the linear mapping is GBP", AnswerPayment[3][4]);
119 //document.write("<br>");
120
121 //Question H1 5
122 if (num <= 0.15) {AnswerPayment[4][3] = 7.5;} else {AnswerPayment[4][3] = 0;}
123 AnswerPayment[4][1] = AnswerPayment[4][3] - Number(AnswerPayment[4][0]);
124 AnswerPayment[4][4] = LinearMap(AnswerPayment[4][1], 0, 50, 0, maxpayment);
125
126 //document.write("lottery 5 outcome is: ", AnswerPayment[4][3], " answer was ",
    AnswerPayment[4][0], " and your losses are: ",
127
128 AnswerPayment[4][1], " and the linear mapping is GBP", AnswerPayment[4][4]);
129 //document.write("<br>");
130
131 //Question H1 6
132 if (num <= ambig0to30) {AnswerPayment[5][3] = 50;} else {AnswerPayment[5][3] =
    0;}
133 AnswerPayment[5][1] = AnswerPayment[5][3] - Number(AnswerPayment[5][0]);
134 AnswerPayment[5][4] = LinearMap(AnswerPayment[5][1], 0, 50, 0, maxpayment);
135
136 //document.write("lottery 6 outcome is: ", AnswerPayment[5][3], " answer was ",
    AnswerPayment[5][0], " and your losses are: ",
137
138 AnswerPayment[5][1], " and the linear mapping is GBP", AnswerPayment[5][4]);
139 //document.write("<br>");
140
141 //Question H1 7
142 if (num <= 0.15) {AnswerPayment[6][3] = ambig20to80;} else {AnswerPayment[6][3]
    = 0;}
143 AnswerPayment[6][1] = AnswerPayment[6][3] - Number(AnswerPayment[6][0]);
144 AnswerPayment[6][4] = LinearMap(AnswerPayment[6][1], 0, 80, 0, maxpayment);
145
146 //document.write("lottery 7 outcome is: ", AnswerPayment[6][3], " answer was ",
    AnswerPayment[6][0], " and your losses are: ",
147
148 AnswerPayment[6][1], " and the linear mapping is GBP", AnswerPayment[6][4]);
149 //document.write("<br>");
```

A.1 Appendix: Experiment 1

```
150
151 //Question H1 8
152 if (num <= ambig0to30) {AnswerPayment[7][3] = ambig20to80;} else {AnswerPayment
    [7][3] = 0;}
153 AnswerPayment[7][1] = AnswerPayment[7][3] - Number(AnswerPayment[7][0]);
154 AnswerPayment[7][4] = LinearMap(AnswerPayment[7][1], 0, 80, 0, maxpayment);
155
156 //document.write("lottery 8 outcome is: ", AnswerPayment[7][3], " answer was ",
    AnswerPayment[7][0], " and your losses are: ",
157
158 AnswerPayment[7][1], " and the linear mapping is GBP", AnswerPayment[7][4]);
159 //document.write("<br>");
160
161 //Question H1 9
162 if (num <= 0.5) {AnswerPayment[8][3] = 25;} else {AnswerPayment[8][3] = 0;}
163 AnswerPayment[8][1] = AnswerPayment[8][3] - Number(AnswerPayment[8][0]);
164 AnswerPayment[8][4] = LinearMap(AnswerPayment[8][1], 0, 50, 0, maxpayment);
165
166 //document.write("lottery 9 outcome is: ", AnswerPayment[8][3], " answer was ",
    AnswerPayment[8][0], " and your losses are: ",
167
168 AnswerPayment[8][1], " and the linear mapping is GBP", AnswerPayment[8][4]);
169 //document.write("<br>");
170
171 //Question H1 10
172 if (num <= ambig35to65) {AnswerPayment[9][3] = 50;} else {AnswerPayment[9][3] =
    0;}
173 AnswerPayment[9][1] = AnswerPayment[9][3] - Number(AnswerPayment[9][0]);
174 AnswerPayment[9][4] = LinearMap(AnswerPayment[9][1], 0, 50, 0, maxpayment);
175
176 //document.write("lottery 10 outcome is: ", AnswerPayment[9][3], " answer was ",
    AnswerPayment[9][0], " and your losses are: ",
177
178 AnswerPayment[9][1], " and the linear mapping is GBP", AnswerPayment[9][4]);
179 //document.write("<br>");
180
181 //Question H1 11
182 if (num <= 0.5) {AnswerPayment[10][3] = ambig20to80;} else {AnswerPayment[10][3]
    = 0;}
183 AnswerPayment[10][1] = AnswerPayment[10][3] - Number(AnswerPayment[10][0]);
184 AnswerPayment[10][4] = LinearMap(AnswerPayment[10][1], 0, 80, 0, maxpayment);
185
186 //document.write("lottery 11 outcome is: ", AnswerPayment[10][3], " answer was
    ", AnswerPayment[10][0], " and your losses are:
187
188 ", AnswerPayment[10][1], " and the linear mapping is GBP", AnswerPayment[10][4])
    ;
189 //document.write("<br>");
190
191 //Question H1 12
192 if (num <= ambig35to65) {AnswerPayment[11][3] = ambig20to80;} else {
    AnswerPayment[11][3] = 0;}
193 AnswerPayment[11][1] = AnswerPayment[11][3] - Number(AnswerPayment[3][0]);
194 AnswerPayment[11][4] = LinearMap(AnswerPayment[11][1], 0, 80, 0, maxpayment);
195
196 //document.write("lottery 12 outcome is: ", AnswerPayment[11][3], " answer was "
    , AnswerPayment[11][0], " and your losses are:
```

A.1 Appendix: Experiment 1

```
197
198 ", AnswerPayment[11][1], " and the linear mapping is GBP", AnswerPayment[11][4])
    ;
199 //document.write("<br>");
200
201 //Question H1 13
202 if (num <= 0.85) {AnswerPayment[12][3] = 50;} else {AnswerPayment[12][3] = 0;}
203 AnswerPayment[12][1] = AnswerPayment[12][3] - Number(AnswerPayment[12][0]); //
    outcome minus WTP
204 AnswerPayment[12][4] = LinearMap(AnswerPayment[12][1], 0, 50, 0, maxpayment);
205
206 //document.write("lottery 13 outcome is: ", AnswerPayment[12][3], " answer was "
    , AnswerPayment[12][0], " and your losses are:
207
208 ", AnswerPayment[12][1], " and the linear mapping is GBP", AnswerPayment[12][4])
    ;
209 //document.write("<br>");
210
211 //Question H1 14
212 if (num <= ambig75to100) {AnswerPayment[13][3] = 50;} else {AnswerPayment[13][3]
    = 0;}
213 AnswerPayment[13][1] = AnswerPayment[13][3] - Number(AnswerPayment[13][0]);
214 AnswerPayment[13][4] = LinearMap(AnswerPayment[13][1], 0, 50, 0, maxpayment);
215
216 //document.write("lottery 14 outcome is: ", AnswerPayment[13][3], " answer was "
    , AnswerPayment[13][0], " and your losses are:
217
218 ", AnswerPayment[13][1], " and the linear mapping is GBP", AnswerPayment[13][4])
    ;
219 //document.write("<br>");
220
221 //Question H1 15
222 if (num <= 0.85) {AnswerPayment[14][3] = ambig20to80;} else {AnswerPayment
    [14][3] = 0;}
223 AnswerPayment[14][1] = AnswerPayment[14][3] - Number(AnswerPayment[14][0]);
224 AnswerPayment[14][4] = LinearMap(AnswerPayment[14][1], 0, 80, 0, maxpayment);
225
226 //document.write("lottery 15 outcome is: ", AnswerPayment[14][3], " answer was "
    , AnswerPayment[14][0], " and your losses are:
227
228 ", AnswerPayment[14][1], " and the linear mapping is GBP", AnswerPayment[14][4])
    ;
229 //document.write("<br>");
230
231 //Question H1 16
232 if (num <= ambig75to100) {AnswerPayment[15][3] = ambig20to80;} else {
    AnswerPayment[15][3] = 0;}
233 AnswerPayment[15][1] = AnswerPayment[15][3] - Number(AnswerPayment[15][0]);
234 AnswerPayment[15][4] = LinearMap(AnswerPayment[15][1], 0, 80, 0, maxpayment);
235
236 //document.write("lottery 16 outcome is: ", AnswerPayment[15][3], " answer was "
    , AnswerPayment[15][0], " and your losses are:
237
238 ", AnswerPayment[15][1], " and the linear mapping is GBP", AnswerPayment[15][4])
    ;
239 //document.write("<br>");
240
```

A.1 Appendix: Experiment 1

```
241 //STORING Question Text for HYPOTHESIS 1
242 AnswerPayment [0] [2] = "${q://QID2/QuestionText}";
243 AnswerPayment [1] [2] = "${q://QID3/QuestionText}";
244 AnswerPayment [2] [2] = "${q://QID5/QuestionText}";
245 AnswerPayment [3] [2] = "${q://QID6/QuestionText}";
246 AnswerPayment [4] [2] = "${q://QID7/QuestionText}";
247 AnswerPayment [5] [2] = "${q://QID8/QuestionText}";
248 AnswerPayment [6] [2] = "${q://QID9/QuestionText}";
249 AnswerPayment [7] [2] = "${q://QID10/QuestionText}";
250 AnswerPayment [8] [2] = "${q://QID11/QuestionText}";
251 AnswerPayment [9] [2] = "${q://QID12/QuestionText}";
252 AnswerPayment [10] [2] = "${q://QID13/QuestionText}";
253 AnswerPayment [11] [2] = "${q://QID14/QuestionText}";
254 AnswerPayment [12] [2] = "${q://QID15/QuestionText}";
255 AnswerPayment [13] [2] = "${q://QID16/QuestionText}";
256 AnswerPayment [14] [2] = "${q://QID17/QuestionText}";
257 AnswerPayment [15] [2] = "${q://QID18/QuestionText}";
258
259 //STORING Question Text for HYPOTHESIS 2
260 AnswerPayment [16] [2] = "${q://QID20/QuestionText}";
261 AnswerPayment [17] [2] = "${q://QID25/QuestionText}";
262 AnswerPayment [18] [2] = "${q://QID179/QuestionText}";
263 AnswerPayment [19] [2] = "${q://QID28/QuestionText}";
264 AnswerPayment [20] [2] = "${q://QID41/QuestionText}";
265
266 AnswerPayment [21] [2] = "${q://QID42/QuestionText}";
267 AnswerPayment [22] [2] = "${q://QID180/QuestionText}";
268 AnswerPayment [23] [2] = "${q://QID173/QuestionText}";
269 AnswerPayment [24] [2] = "${q://QID256/QuestionText}";
270
271 AnswerPayment [25] [2] = "omitted";
272 AnswerPayment [26] [2] = "omitted";
273
274 //ASSIGNING ANSWERED VALUES TO AnswerPayment ARRAY, FOR HYPOTHESIS 2 (9 Slots:
    from 16 to 24)
275 AnswerPayment [16] [0] = "${e://Field/H2Answer1}";
276 AnswerPayment [17] [0] = "${e://Field/H2Answer2}";
277 AnswerPayment [18] [0] = "${e://Field/H2Answer3}";
278 AnswerPayment [19] [0] = "${e://Field/H2Answer4}";
279 AnswerPayment [20] [0] = "${e://Field/H2Answer5}";
280
281 AnswerPayment [21] [0] = "${e://Field/H2Answer6}";
282 AnswerPayment [22] [0] = "${e://Field/H2Answer7}";
283 AnswerPayment [23] [0] = "${e://Field/H2Answer8}";
284 AnswerPayment [24] [0] = "${e://Field/H2Answer9}";
285
286 AnswerPayment [25] [0] = "omitted";
287 AnswerPayment [26] [0] = "omitted";
288
289
290 //ASSIGNING PAYMENTS FOR HYPOTHESIS 2
291
292 //Question H2 1
293 if (String(AnswerPayment [16] [0]) === "A") //Lottery 9
294 {
295   if (num <= 0.85) {AnswerPayment [16] [3] = 45;}
296   else if (num > 0.85 && num <=0.93) {AnswerPayment [16] [3] = 220;}
```

A.1 Appendix: Experiment 1

```
297 else if (num > 0.93 && num <=0.965) {AnswerPayment[16][3] = 300;}
298 else if (num > 0.965 && num <=0.99) {AnswerPayment[16][3] = 450;}
299 else {AnswerPayment[16][3] = 900;}
300
301 AnswerPayment[16][4] = LinearMap(AnswerPayment[16][3], 0, 1000, 0, maxpayment);
302 }
303 else //if (String(AnswerPayment[24][0]) === "B"); //Lottery 10
304 {
305 if (num <= 0.85) {AnswerPayment[16][3] = 50;}
306 else if (num > 0.85 && num <=0.93) {AnswerPayment[16][3] = 150;}
307 else if (num > 0.93 && num <=0.965) {AnswerPayment[16][3] = 300;}
308 else if (num > 0.965 && num <=0.99) {AnswerPayment[16][3] = 450;}
309 else {AnswerPayment[16][3] = 1000;}
310
311 AnswerPayment[16][4] = LinearMap(AnswerPayment[16][3], 0, 1000, 0, maxpayment);
312 }
313 AnswerPayment[16][1] = maxpayment - AnswerPayment[16][4]; // maximum additional
    payment minus random outcome
314
315 //document.write("You preferred lottery ", AnswerPayment[16][0]," the random
    outcome of lottery H2 10 is: -", AnswerPayment[16]
316
317 [3], " and the linear mapping is GBP", AnswerPayment[16][4], " and your
    additional payment is GBP", AnswerPayment[16][1]);
318 //document.write("<br>");
319
320
321 //Question H2 2
322 if (String(AnswerPayment[17][0]) === "A") //Lottery 10
323 {
324 if (num <= 0.85) {AnswerPayment[17][3] = 50;}
325 else if (num > 0.85 && num <=0.93) {AnswerPayment[17][3] = 170;}
326 else if (num > 0.93 && num <=0.965) {AnswerPayment[17][3] = 300;}
327 else if (num > 0.965 && num <=0.99) {AnswerPayment[17][3] = 400;}
328 else {AnswerPayment[17][3] = 1000;}
329
330 AnswerPayment[17][4] = LinearMap(AnswerPayment[17][3], 0, 1000, 0, maxpayment);
331 }
332 else //if (String(AnswerPayment[17][0]) === "B"); //Lottery 11
333 {
334 if (num <= 0.85) {AnswerPayment[17][3] = 45;}
335 else if (num > 0.85 && num <=0.93) {AnswerPayment[17][3] = 250;}
336 else if (num > 0.93 && num <=0.965) {AnswerPayment[17][3] = 350;}
337 else if (num > 0.965 && num <=0.99) {AnswerPayment[17][3] = 450;}
338 else {AnswerPayment[17][3] = 800;}
339
340 AnswerPayment[17][4] = LinearMap(AnswerPayment[17][3], 0, 1000, 0, maxpayment);
341 }
342 AnswerPayment[17][1] = maxpayment - AnswerPayment[17][4];
343
344 //document.write("You preferred lottery ", AnswerPayment[17][0]," the random
    outcome of lottery H2 10 is: -", AnswerPayment[17]
345
346 [3], " and the linear mapping is GBP", AnswerPayment[17][4], " and your
    additional payment is GBP", AnswerPayment[17][1]);
347 //document.write("<br>");
348
```

A.1 Appendix: Experiment 1

```
349
350 //Question H2 3
351 if (String(AnswerPayment[18][0]) === "A") //Lottery 8
352 {
353   if (num <= 0.15) {AnswerPayment[18][3] = 0;}
354   else if (num > 0.15 && num <=0.45) {AnswerPayment[18][3] = 200;}
355   else if (num > 0.45 && num <=0.75) {AnswerPayment[18][3] = 300;}
356   else if (num > 0.75 && num <=0.95) {AnswerPayment[18][3] = 450;}
357   else {AnswerPayment[18][3] = 700;}
358
359   AnswerPayment[18][4] = LinearMap(AnswerPayment[18][3], 0, 700, 0, maxpayment);
360 }
361 else //if (String(AnswerPayment[18][0]) === "B"); //Lottery 6
362 {
363   if (num <= 0.15) {AnswerPayment[18][3] = 0;}
364   else if (num > 0.15 && num <=0.45) {AnswerPayment[18][3] = 166.66;}
365   else if (num > 0.45 && num <=0.75) {AnswerPayment[18][3] = 300;}
366   else if (num > 0.75 && num <=0.95) {AnswerPayment[18][3] = 450;}
367   else {AnswerPayment[18][3] = 900;}
368
369   AnswerPayment[18][4] = LinearMap(AnswerPayment[18][3], 0, 900, 0, maxpayment);
370 }
371 AnswerPayment[18][1] = maxpayment - AnswerPayment[18][4];
372
373 //document.write("You preferred lottery ", AnswerPayment[18][0]," the random
      outcome of lottery H2 10 is: -", AnswerPayment[18]
374
375 [3], " and the linear mapping is GBP", AnswerPayment[18][4], " and your
      additional payment is GBP", AnswerPayment[18][1]);
376 //document.write("<br>");
377
378
379 //Question H2 4
380 if (String(AnswerPayment[19][0]) === "A") //Lottery 6
381 {
382   if (num <= 0.15) {AnswerPayment[19][3] = 0;}
383   else if (num > 0.15 && num <=0.45) {AnswerPayment[19][3] = 166.66;}
384   else if (num > 0.45 && num <=0.75) {AnswerPayment[19][3] = 300;}
385   else if (num > 0.75 && num <=0.95) {AnswerPayment[19][3] = 450;}
386   else {AnswerPayment[19][3] = 900;}
387
388   AnswerPayment[19][4] = LinearMap(AnswerPayment[19][3], 0, 900, 0, maxpayment);
389 }
390 else //if (String(AnswerPayment[19][0]) === "B"); //Lottery 7
391 {
392   if (num <= 0.15) {AnswerPayment[19][3] = 0;}
393   else if (num > 0.15 && num <=0.45) {AnswerPayment[19][3] = 183.33;}
394   else if (num > 0.45 && num <=0.75) {AnswerPayment[19][3] = 300;}
395   else if (num > 0.75 && num <=0.95) {AnswerPayment[19][3] = 450;}
396   else {AnswerPayment[19][3] = 800;}
397
398   AnswerPayment[19][4] = LinearMap(AnswerPayment[19][3], 0, 800, 0, maxpayment);
399 }
400 AnswerPayment[19][1] = maxpayment - AnswerPayment[19][4];
401
402 //document.write("You preferred lottery ", AnswerPayment[19][0]," the random
      outcome of lottery H2 10 is: -", AnswerPayment[19]
```

A.1 Appendix: Experiment 1

```
403
404 [3], " and the linear mapping is GBP", AnswerPayment[19][4], " and your
      additional payment is GBP", AnswerPayment[19][1]);
405 //document.write("<br>");
406
407
408 //Question H2 5
409 if (String(AnswerPayment[20][0]) === "A") //Lottery 4
410 {
411   if (num <= 0.85) {AnswerPayment[20][3] = 50;}
412   else if (num > 0.85 && num <=0.93) {AnswerPayment[20][3] = 150;}
413   else if (num > 0.93 && num <=0.965) {AnswerPayment[20][3] = 300;}
414   else if (num > 0.965 && num <=0.99) {AnswerPayment[20][3] = 450;}
415   else {AnswerPayment[20][3] = 1000;}
416
417   AnswerPayment[20][4] = LinearMap(AnswerPayment[20][3], 0, 1000, 0, maxpayment);
418 }
419 else //if (String(AnswerPayment[20][0]) === "B";) Lottery 10_old
420 {
421   if (num <= 0.85) {AnswerPayment[20][3] = 46;}
422   else if (num > 0.85 && num <=0.93) {AnswerPayment[20][3] = 180;}
423   else if (num > 0.93 && num <=0.965) {AnswerPayment[20][3] = 350;}
424   else if (num > 0.965 && num <=0.99) {AnswerPayment[20][3] = 480;}
425   else {AnswerPayment[20][3] = 900;}
426
427   AnswerPayment[20][4] = LinearMap(AnswerPayment[20][3], 0, 800, 0, maxpayment);
428 }
429 AnswerPayment[20][1] = maxpayment - AnswerPayment[20][4];
430
431 //document.write("You preferred lottery ", AnswerPayment[20][0]," the random
      outcome of lottery H2 10 is: -", AnswerPayment[20]
432
433 [3], " and the linear mapping is GBP", AnswerPayment[20][4], " and your
      additional payment is GBP", AnswerPayment[20][1]);
434 //document.write("<br>");
435
436
437
438 var TotalDuration = "${e://Field/Q_TotalDuration}"; //is an integer indicating
      seconds
439 var TotalDuration_min = Math.round((TotalDuration/60)*10)/10;
440
441 var RandomNumber = 16 + Math.floor((Math.random()*5)); //old approach: n=23 is
      for the first 23 questions, but now I choose
442
443 between H2 1 and H2 5
444
445 var FinalPayment = maxpayment - Math.abs(Number(AnswerPayment[RandomNumber][4]))
      ;
446
447 if (FinalPayment >= 0 && FinalPayment <= maxpayment)
448 {
449   Qualtrics.SurveyEngine.setEmbeddedData('YourPayment', Math.round(FinalPayment
      *100)/100);
450 }
451 else //if (Payment < 0)
452 {
```

A.1 Appendix: Experiment 1

```
453 var zero = 0;
454 Qualtrics.SurveyEngine.setEmbeddedData('YourPayment',zero);
455 }
456 var FeeAndAdditionalPayment = participationfee + FinalPayment;
457 Qualtrics.SurveyEngine.setEmbeddedData('YourFeeAndAdditionalPayment',
    FeeAndAdditionalPayment);
458
459 Qualtrics.SurveyEngine.setEmbeddedData('ChosenQuestion',RandomNumber+1);
460 Qualtrics.SurveyEngine.setEmbeddedData('MaximumPayment',maxpayment);
461 Qualtrics.SurveyEngine.setEmbeddedData('YourParticipationFee',participationfee);
462 Qualtrics.SurveyEngine.setEmbeddedData('YourTotalDuration',TotalDuration_min);
463
464 Qualtrics.SurveyEngine.setEmbeddedData('ChosenQuestionAnswer',AnswerPayment[
    RandomNumber][0]);
465 Qualtrics.SurveyEngine.setEmbeddedData('ChosenQuestionLosses',AnswerPayment[
    RandomNumber][4]);
466 Qualtrics.SurveyEngine.setEmbeddedData('ChosenQuestionText',AnswerPayment[
    RandomNumber][2]);
467 Qualtrics.SurveyEngine.setEmbeddedData('ChosenQuestionOutcome',AnswerPayment[
    RandomNumber][3]);
468
469 Qualtrics.SurveyEngine.setEmbeddedData('enum',num);
470 Qualtrics.SurveyEngine.setEmbeddedData('eambig0to10',ambig0to10);
471 Qualtrics.SurveyEngine.setEmbeddedData('eambig0to30',ambig0to30);
472 Qualtrics.SurveyEngine.setEmbeddedData('eambig35to65',ambig35to65);
473 Qualtrics.SurveyEngine.setEmbeddedData('eambig75to100',ambig75to100);
474 Qualtrics.SurveyEngine.setEmbeddedData('eambig20to80',ambig20to80);
475
476 //document.write("RandomNumber+1: ", RandomNumber+1);
477 //document.write("<br>");
478 //document.write("from randomness: ", num);
479 //document.write("<br>");
480 //document.write("AnswerPayment[RandomNumber][0]: ", AnswerPayment[RandomNumber
    ][0]);
481 //document.write("<br>");
482 //document.write("AnswerPayment[RandomNumber][1]: ", AnswerPayment[RandomNumber
    ][1]);
483 //document.write("<br>");
484 //document.write("AnswerPayment[RandomNumber][2]: ", AnswerPayment[RandomNumber
    ][2]);
485 //document.write("<br>");
486 //document.write("AnswerPayment[RandomNumber][2]: ", AnswerPayment[RandomNumber
    ][2]);
487 //document.write("<br>");
488 //document.write("AnswerPayment[RandomNumber][2]: ", AnswerPayment[RandomNumber
    ][2]);
489 //document.write("<br>");
490
491
492 this.hideNextButton();
493 this.showNextButton.delay(3);
494 });
```


A.1.8 Experiment Analysis

A.1.9 Data Cleaning

Data analysis was conducted using SPSS version 21 [1] and data cleaning consisted of the following actions:

1. There were two datasets collected for the purposes of this experiment. The first dataset was collected between 21/05 and 11/06/2014 and it was targeted at alumni and MSc students at Royal Holloway. The majority of the participants are information security professionals. The second sample was collected on 26/08/2014 and was targeted at the student database of the Laboratory for Decision Making and Economic Research at Royal Holloway, University of London. The majority of this sample consisted of individuals that are not related to information security. Datasets were combined.
2. A filter was implemented by the use of the willingness to pay (WTP) questions of Table A.1. Half questions of the table have a maximum monetary loss of 50 USD and the other half a maximum loss of 80 USD. Replies with values greater than fifty and eighty dollars respectively, have been excluded from the analysis of the corresponding lotteries. Only a few cases were excluded from the analysis by using this filter, by being considered invalid; in all these cases, there were consecutive willingness to pay choices to avoid lotteries that were larger than the maximum potential loss.
3. All missing cases were excluded. These were caused either by subjects that aborted the experiments half-way or subjects that happened to be online when the experiment became inactive.

The final valid number of cases was $N_1 = 59$ for professionals, $N_2 = 58$ for students, and $N = 117$ for the merged dataset.

An additional validity check was conducted on the significance of the variable *mother tongue*, to see whether non-native English speakers had any issues with understanding instructions or questions. No language effect was found in the data.

A.1.10 Outliers

For testing whether there is a significant number of outliers in the sample, we used the following method. The z-scores were computed for all WTP questions of variables H_{1i} and H_{2j} . Then the cumulative percentage of cases that had a standard deviation that was larger in absolute value than 1.96 was computed. If this percentage constituted more than 0.05 of the total cases, then there would be more outliers in the distribution of the given variable than we would expect in a normal distribution. It was however important that this analysis was conducted separately for professionals and students, so that we can exclude the possibility of having the sample type act as a moderator; for this reason the merged dataset was split into two. We should state that no outliers were excluded by this methodology, the purpose of which was to examine their distribution.

The analysis revealed six out of the fifteen variables ($H_{11}, H_{12}, H_{13}, H_{14}, H_{17}$ and H_{28}) with outlier percentages more than the expected. However, at closer examination we observed that this deviation was caused by one or two large values in the whole sample. Moreover, the aforementioned variables either had only one or no extreme values ($|z| > 3.29$) and the majority of potential outliers was in the range of $|z| \in (1.96, 2.58)$ or $|z| \in (2.58, 3.29)$. Therefore, the existence and distribution of outliers can be considered roughly within the expected ranges of a normal distribution. This means that existence of outliers was at the edge of being considered significant, and the following statistical tests on the data could be conducted without considering additional “without-outlier” analyses.

It is also worth noting that the deviation from normality by outlier values was mainly observed in the lotteries with low expected value where higher WTP values could occur more easily.

Table A.2 contains the percentages of the values that are potential outliers for all outcome variables, split into students and professionals. Cumulative percent denotes the exact portion of data cases that have z-scores, such that $|z| > 1.96$. Valid percent is the portion of cases in the range $1.96 < |z| < 2.58$. So, a difference between valid and cumulative percentage implies the existence of more extreme outliers, i.e. with z-scores $|z| > 2.58$.

A.1 Appendix: Experiment 1

Table A.2: Potential Outliers ($|z| > 1.96$) for the z-scores of all outcome variables

Variable	Students		Professionals	
	Valid Percent	Cumulative Percent	Valid Percent	Cumulative Percent
H_11	1.7	6.9	3.4	6.8
H_12	8.6	10.3	3.4	5.1
H_13	1.7	5.2	5.6	7.4
H_14	5.2	6.9	1.7	3.4
H_15	3.4	6.9	1.7	6.8
H_16	1.7	5.2	3.7	3.7
H_17	3.4	5.2	1.7	3.4
H_18	1.7	5.2	1.7	3.4
H_19	5.2	5.2	5.1	6.8
H_110	5.2	5.2	5.1	5.1
H_111	1.7	3.4	5.1	6.8
H_112	1.7	3.4	1.7	3.4
H_26	1.7	3.4	3.4	6.8
H_27	3.4	6.9	3.4	5.1
H_28	1.7	6.9	3.4	5.1

A.1.11 Controlling for Order Effects

Before measuring the actual attitudes on risky and ambiguous lotteries, we examined data for potential order effects. In order to control for potential order effects in the series of H_1i instrument variables, two conditions were created in the experiment, one presenting the risky lotteries first and then progressing to the ambiguous lotteries and another condition with the opposite order.

Subjects were randomly assigned to one of these two conditions. The first group was named *Risk-to-Ambiguity* group, was marked with a dummy variable $RISK_FIRST = 1$, and presented questions H_11 , H_15 , H_19 , H_13 , H_17 , H_111 first. The second group, the *Ambiguity-to-Risk* one, consisted of lottery-questions H_14 , H_18 , H_112 , H_12 , H_16 , H_110 , followed by the lotteries of the first group. Since there are two conditions with different subjects, analysis on these two groups was conducted by the non-parametric Mann-Whitney test, and the sample was split into professionals and students, using a filter variable that asks participants whether they are related to the information security profession.

Both professionals and students samples were found free of any order effect between risk and ambiguity, as there was no statistically significant difference between the two condition groups (Table A.3).

A.1 Appendix: Experiment 1

Table A.3: Mann-Whitney U Test for Order Effects

		Students N=58	Professionals N=59
H_11	Test Statistic Sig. (2-tailed)	377 .499	294 .219
H_12	Test Statistic Sig. (2-tailed)	336 .188	259 .064
H_13	Test Statistic Sig. (2-tailed)	432.5 .845	369 .313
H_14	Test Statistic Sig. (2-tailed)	423.5 .956	341 .150
H_15	Test Statistic Sig. (2-tailed)	398 .731	383.5 .430
H_16	Test Statistic Sig. (2-tailed)	387.5 .611	342 .156
H_17	Test Statistic Sig. (2-tailed)	506 .177	405.5 .653
H_18	Test Statistic Sig. (2-tailed)	439.5 .761	375.5 .364
H_19	Test Statistic Sig. (2-tailed)	481 .336	381.5 .406
H_110	Test Statistic Sig. (2-tailed)	468.5 .448	466 .637
H_111	Test Statistic Sig. (2-tailed)	452.5 .611	379.5 .398
H_112	Test Statistic Sig. (2-tailed)	497 .230	401 .605

Is distribution of H_1i the same across categories of
 “Risky questions presented before Ambiguity questions”?
 Null hypothesis is retained for all variables, for both samples.

A.1 Appendix: Experiment 1

A.1.12 Mathematica Code

The following calculations were used in Experiment 1 and were conducted with Mathematica version 9.0 [2].

A.1.12.1 Saliency Calculations of L6 VS L7 with Graph

```
LotteryA = {{0, -166.66, -300, -450, -900}}
LotteryB = {{0, -183.33, -300, -450, -800}}
P = {{0.15, 0.30, 0.30, 0.20, 0.05}}
 $\theta = 0.1$ 
 $\sigma[x_, y_] := (\text{Abs}[x - y]) / (\text{Abs}[x] + \text{Abs}[y] + \theta)$ 

(* calculate a table with all  $\sigma$ 's // N[] is for decimal numbers *)
s = Table[N[ $\sigma$ [LotteryA[[1, i]], LotteryB[[1, j]]]], {i, 1, 5}, {j, 1, 5}]
(* calculate a table with all plain outcome differences *)
 $\Delta v = \text{Table}[\text{LotteryA}[[1, i]] - \text{LotteryB}[[1, j]], \{i, 1, 5\}, \{j, 1, 5\}]$ 

Print["***** This is the list of
      all (1) saliencies, (2)  $\Delta v$ 's and (3) probabilities: "]
s2 = Flatten[ArrayReshape[s, {1, 25}]]
 $\Delta v2 = \text{Flatten}[\text{ArrayReshape}[\Delta v, \{1, 25\}]]$ 
Pm = Flatten[List[P, {{P[[1, 2]], P[[1, 2]], P[[1, 3]], P[[1, 4]], P[[1, 5]]},
  {{P[[1, 3]], P[[1, 3]], P[[1, 3]], P[[1, 4]], P[[1, 5]]},
  {{P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 5]]},
  {{P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]]}]]]
Print["The most salient pair is :  $\sigma =$ ", Max[s]]

Print["***** This is the ordering of the
      saliency elements of table s2 (smallest to largest):"]
s2ordered = Ordering[s2]
k = Range[25, 1, -1]

(* with various  $\delta$ s ---
   can find  $\delta$  which is switching point of preference between Lottery A and B *)
Print["Calculations for A=L10 and B=L11 for a
      range of  $\delta$ 's (positive values imply that L10 > L11) "]
 $\Sigma 2 = \text{Table}[\text{Total}[\text{Table}[Pm[[s2ordered[[i]]]] * \Delta v2[[s2ordered[[i]]]] * d^k[[i]],
  \{i, 25, 1, -1\}]], \{d, 0, 1, 0.01\}]$ 
ListPlot[ $\Sigma 2$ , DataRange -> {0, 1}, Filling -> Axis, AspectRatio -> 1/1,
  AxesOrigin -> {0, 0}, AxesLabel -> { $\delta$ , "Sum (9)"},
  LabelStyle -> Directive[Black, Large]]

{{0, -166.66, -300, -450, -900}}
{{0, -183.33, -300, -450, -800}}
{{0.15, 0.3, 0.3, 0.2, 0.05}}
0.1
{0., 0.999455, 0.999667, 0.999778, 0.999875},
{0.9994, 0.0476163, 0.285671, 0.459401, 0.655116},
{0.999667, 0.241338, 0., 0.199973, 0.454504},
{0.999778, 0.420994, 0.199973, 0., 0.279978},
{0.999889, 0.661483, 0.499958, 0.333309, 0.0588201}}
```

A.1 Appendix: Experiment 1

2 | *Saliency calculations L6 VS L7 graph_FontLabel.nb*

```
{0, 183.33, 300, 450, 800},
{-166.66, 16.67, 133.34, 283.34, 633.34}, {-300, -116.67, 0, 150, 500},
{-450, -266.67, -150, 0, 350}, {-900, -716.67, -600, -450, -100}}

***** This is the list of all (1) saliencies, (2)  $\Delta v$ 's and (3) probabilities:
{0., 0.999455, 0.999667, 0.999778, 0.999875, 0.9994,
0.0476163, 0.285671, 0.459401, 0.655116, 0.999667, 0.241338,
0., 0.199973, 0.454504, 0.999778, 0.420994, 0.199973, 0.,
0.279978, 0.999889, 0.661483, 0.499958, 0.333309, 0.0588201}

{0, 183.33, 300, 450, 800, -166.66, 16.67, 133.34, 283.34, 633.34, -300, -116.67,
0, 150, 500, -450, -266.67, -150, 0, 350, -900, -716.67, -600, -450, -100}

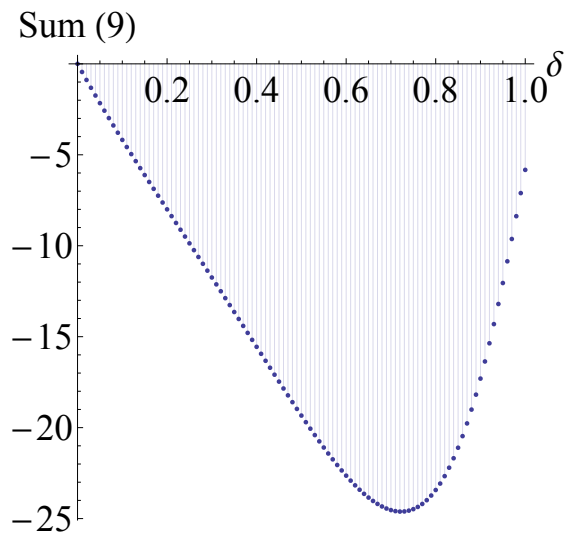
{0.15, 0.3, 0.3, 0.2, 0.05, 0.3, 0.3, 0.3, 0.2, 0.05, 0.3, 0.3, 0.3,
0.2, 0.05, 0.2, 0.2, 0.2, 0.2, 0.05, 0.05, 0.05, 0.05, 0.05, 0.05}

The most salient pair is :  $\sigma = 0.999889$ 

***** This is the ordering of
the saliency elements of table s2 (smallest to largest):
{1, 13, 19, 7, 25, 14, 18, 12, 20, 8,
24, 17, 15, 9, 23, 10, 22, 6, 2, 3, 11, 4, 16, 5, 21}

{25, 24, 23, 22, 21, 20, 19, 18, 17, 16,
15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1}

Calculations for A=L10 and B=L11 for
a range of  $\delta$ 's (positive values imply that L10 > L11)
{0., -0.446089, -0.884706, -1.31636, -1.74154, -2.16071, -2.57434, -2.98285,
-3.38666, -3.78619, -4.18181, -4.57389, -4.96281, -5.3489, -5.7325, -6.11392,
-6.49346, -6.87142, -7.24807, -7.62367, -7.99848, -8.37272, -8.74661,
-9.12035, -9.49413, -9.86812, -10.2425, -10.6173, -10.9928, -11.3689,
-11.7459, -12.1237, -12.5023, -12.8818, -13.2622, -13.6434, -14.0253,
-14.4078, -14.7909, -15.1744, -15.558, -15.9415, -16.3248, -16.7075,
-17.0892, -17.4697, -17.8484, -18.2251, -18.5991, -18.9699, -19.3371,
-19.6998, -20.0576, -20.4096, -20.755, -21.0931, -21.423, -21.7437, -22.0542,
-22.3535, -22.6404, -22.9138, -23.1724, -23.4148, -23.6397, -23.8455,
-24.0308, -24.1939, -24.3332, -24.4468, -24.5329, -24.5896, -24.6148,
-24.6067, -24.5629, -24.4814, -24.3599, -24.1962, -23.9881, -23.7333,
-23.4295, -23.0747, -22.6667, -22.2036, -21.6835, -21.1051, -20.4668,
-19.7679, -19.0078, -18.1863, -17.3041, -16.3622, -15.3626, -14.308,
-13.2021, -12.0496, -10.8562, -9.62881, -8.37554, -7.10564, -5.8295}
```



A.1 Appendix: Experiment 1

A.1.12.2 Saliency Calculations of L10 VS L11 with Graph

```
LotteryA = {{-50, -170, -300, -400, -1000}}
LotteryB = {{-45, -250, -350, -450, -800}}
P = {{0.85, 0.08, 0.035, 0.025, 0.01}}
 $\theta = 0.1$ 
 $\sigma[x_, y_] := (\text{Abs}[x - y]) / (\text{Abs}[x] + \text{Abs}[y] + \theta)$ 

(* calculate a table with all  $\sigma$ 's // N[] is for decimal numbers *)
s = Table[N[ $\sigma$ [LotteryA[[1, i]], LotteryB[[1, j]]]], {i, 1, 5}, {j, 1, 5}]
(* calculate a table with all plain outcome differences *)
 $\Delta v = \text{Table}[\text{LotteryA}[[1, i]] - \text{LotteryB}[[1, j]], \{i, 1, 5\}, \{j, 1, 5\}]$ 

Print["***** This is the list of
      all (1) saliences, (2)  $\Delta v$ 's and (3) probabilities: "]
s2 = Flatten[ArrayReshape[s, {1, 25}]]
 $\Delta v2 = \text{Flatten}[\text{ArrayReshape}[\Delta v, \{1, 25\}]]$ 
Pm = Flatten[List[P, {P[[1, 2]], P[[1, 2]], P[[1, 3]], P[[1, 4]], P[[1, 5]]}],
             {{P[[1, 3]], P[[1, 3]], P[[1, 3]], P[[1, 4]], P[[1, 5]]}},
             {{P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 5]]}},
             {{P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]]}}]
Print["The most salient pair is :  $\sigma =$ ", Max[s]]

Print["***** This is the ordering of the
      salience elements of table s2 (smallest to largest):"]
s2ordered = Ordering[s2]
k = Range[25, 1, -1]

(* with various  $\delta$ s ---
   can find  $\delta$  which is switching point of preference between Lottery A and B *)
Print["Calculations for A=L10 and B=L11 for a
      range of  $\delta$ 's (positive values imply that L10 > L11) "]
 $\Sigma 2 = \text{Table}[\text{Total}[\text{Table}[Pm[[s2ordered[[i]]]] * \Delta v2[[s2ordered[[i]]]] * d^k[[i]]],
                 \{i, 25, 1, -1\}], \{d, 0, 1, 0.01\}]$ 
ListPlot[ $\Sigma 2$ , DataRange -> {0, 1}, Filling -> Axis, AspectRatio -> 1 / 1,
         AxesLabel -> { $\delta$ , "Sum (9)"}, LabelStyle -> Directive[Black, Large]]

{{-50, -170, -300, -400, -1000}}
{{-45, -250, -350, -450, -800}}
{{0.85, 0.08, 0.035, 0.025, 0.01}}
0.1
{0.0525762, 0.666445, 0.749813, 0.79984, 0.882249},
{0.581125, 0.190431, 0.346087, 0.45154, 0.649418},
{0.738916, 0.0908926, 0.0769112, 0.199973, 0.454504},
{0.797574, 0.230734, 0.0666578, 0.0588166, 0.333306},
{0.913788, 0.599952, 0.481446, 0.379284, 0.111105}
{-5, 200, 300, 400, 750}, {-125, 80, 180, 280, 630}, {-255, -50, 50, 150, 500},
{-355, -150, -50, 50, 400}, {-955, -750, -650, -550, -200}

***** This is the list of all (1) saliences, (2)  $\Delta v$ 's and (3) probabilities:
```


A.1 Appendix: Experiment 1

2 | *Saliency calculations L10 VS L11 graph_FontLabel.nb*

```
{0.0525762, 0.666445, 0.749813, 0.79984, 0.882249, 0.581125,
 0.190431, 0.346087, 0.45154, 0.649418, 0.738916, 0.0908926,
 0.0769112, 0.199973, 0.454504, 0.797574, 0.230734, 0.0666578,
 0.0588166, 0.333306, 0.913788, 0.599952, 0.481446, 0.379284, 0.111105}

{-5, 200, 300, 400, 750, -125, 80, 180, 280, 630, -255, -50, 50,
 150, 500, -355, -150, -50, 50, 400, -955, -750, -650, -550, -200}

{0.85, 0.08, 0.035, 0.025, 0.01, 0.08, 0.08, 0.035, 0.025, 0.01, 0.035, 0.035,
 0.035, 0.025, 0.01, 0.025, 0.025, 0.025, 0.025, 0.01, 0.01, 0.01, 0.01, 0.01}

The most salient pair is :  $\sigma = 0.913788$ 

***** This is the ordering of
the saliency elements of table s2 (smallest to largest):

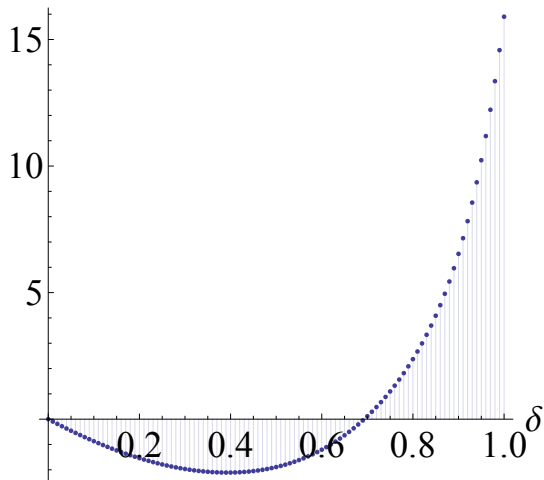
{1, 19, 18, 13, 12, 25, 7, 14, 17, 20,
 8, 24, 9, 15, 23, 6, 22, 10, 2, 11, 3, 16, 4, 5, 21}

{25, 24, 23, 22, 21, 20, 19, 18, 17, 16,
 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1}

Calculations for A=L10 and B=L11 for
a range of  $\delta$ 's (positive values imply that L10 > L11)

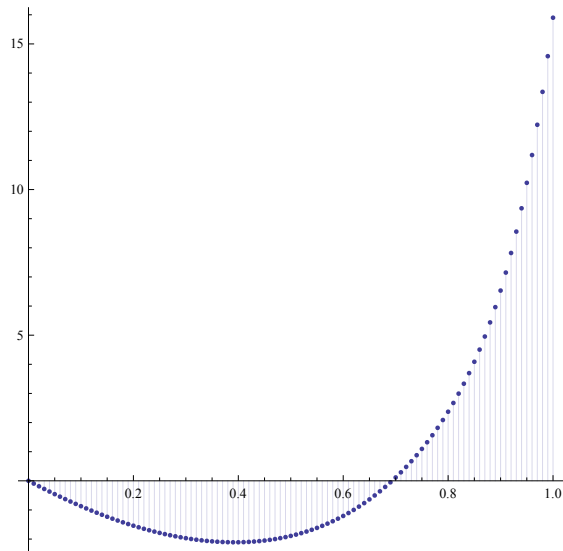
{0., -0.0947401, -0.187921, -0.279487, -0.369382, -0.457552, -0.543947,
-0.628516, -0.711211, -0.791984, -0.87079, -0.947583, -1.02232, -1.09496,
-1.16545, -1.23377, -1.29986, -1.36369, -1.42521, -1.4844, -1.5412,
-1.59557, -1.64749, -1.6969, -1.74377, -1.78806, -1.82972, -1.86871,
-1.90498, -1.93848, -1.96918, -1.99701, -2.02193, -2.04388, -2.0628,
-2.07863, -2.09131, -2.10076, -2.10692, -2.10971, -2.10906, -2.10487,
-2.09706, -2.08553, -2.0702, -2.05095, -2.02767, -2.00026, -1.9686,
-1.93256, -1.89201, -1.84681, -1.79683, -1.74193, -1.68194, -1.61672,
-1.5461, -1.46991, -1.38799, -1.30015, -1.2062, -1.10596, -0.999228,
-0.885789, -0.765429, -0.637918, -0.503012, -0.360453, -0.209959,
-0.0512282, 0.116074, 0.292315, 0.477909, 0.673318, 0.879071, 1.09577,
1.3241, 1.56488, 1.81901, 2.08757, 2.3718, 2.67315, 2.99328, 3.33412,
3.69789, 4.08713, 4.50475, 4.95406, 5.4388, 5.96313, 6.5317, 7.14962,
7.82243, 8.55605, 9.35671, 10.2308, 11.1845, 12.224, 13.3542, 14.579, 15.9}
```

Sum (9)



A.1 Appendix: Experiment 1

```
Calculations for A=L10 and B=L11 for a range
of  $\delta$ 's from 0 to 1 (positive values imply that L10 > L11)
{0., -0.0947401, -0.187921, -0.279487, -0.369382, -0.457552, -0.543947,
-0.628516, -0.711211, -0.791984, -0.87079, -0.947583, -1.02232, -1.09496,
-1.16545, -1.23377, -1.29986, -1.36369, -1.42521, -1.4844, -1.5412,
-1.59557, -1.64749, -1.6969, -1.74377, -1.78806, -1.82972, -1.86871,
-1.90498, -1.93848, -1.96918, -1.99701, -2.02193, -2.04388, -2.0628,
-2.07863, -2.09131, -2.10076, -2.10692, -2.10971, -2.10906, -2.10487,
-2.09706, -2.08553, -2.0702, -2.05095, -2.02767, -2.00026, -1.9686,
-1.93256, -1.89201, -1.84681, -1.79683, -1.74193, -1.68194, -1.61672,
-1.5461, -1.46991, -1.38799, -1.30015, -1.2062, -1.10596, -0.999228,
-0.885789, -0.765429, -0.637918, -0.503012, -0.360453, -0.209959,
-0.0512282, 0.116074, 0.292315, 0.477909, 0.673318, 0.879071, 1.09577,
1.3241, 1.56488, 1.81901, 2.08757, 2.3718, 2.67315, 2.99328, 3.33412,
3.69789, 4.08713, 4.50475, 4.95406, 5.4388, 5.96313, 6.5317, 7.14962,
7.82243, 8.55605, 9.35671, 10.2308, 11.1845, 12.224, 13.3542, 14.579, 15.9}
```



A.1 Appendix: Experiment 1

A.1.12.3 Salience Calculations of L8 VS L6 with Graph

```
LotteryA = {{0, -200, -300, -450, -700}}
LotteryB = {{0, -166.66, -300, -450, -900}}
P = {{0.15, 0.30, 0.30, 0.20, 0.05}}
 $\theta = 0.1$ 
 $\sigma[x_, y_] := (\text{Abs}[x - y]) / (\text{Abs}[x] + \text{Abs}[y] + \theta)$ 

(* calculate a table with all  $\sigma$ 's // N[] is for decimal numbers *)
s = Table[N[ $\sigma$ [LotteryA[[1, i]], LotteryB[[1, j]]]], {i, 1, 5}, {j, 1, 5}]
(* calculate a table with all plain outcome differences *)
 $\Delta v = \text{Table}[\text{LotteryA}[[1, i]] - \text{LotteryB}[[1, j]], \{i, 1, 5\}, \{j, 1, 5\}]$ 

Print["***** This is the list of
      all (1) saliences, (2)  $\Delta v$ 's and (3) probabilities: "]
s2 = Flatten[ArrayReshape[s, {1, 25}]]
 $\Delta v2 = \text{Flatten}[\text{ArrayReshape}[\Delta v, \{1, 25\}]]$ 
Pm = Flatten[List[P, {{P[[1, 2]], P[[1, 2]], P[[1, 3]], P[[1, 4]], P[[1, 5]]}},
             {{P[[1, 3]], P[[1, 3]], P[[1, 3]], P[[1, 4]], P[[1, 5]]}},
             {{P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 5]]}},
             {{P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]]}}]]
Print["The most salient pair is :  $\sigma =$ ", Max[s]]

Print["***** This is the ordering of the
      salience elements of table s2 (smallest to largest):"]
s2ordered = Ordering[s2]
k = Range[25, 1, -1]

(* with various  $\delta$ s ---
   can find  $\delta$  which is switching point of preference between Lottery A and B *)
Print["Calculations for A=L10 and B=L11 for a
      range of  $\delta$ 's (positive values imply that L10 > L11) "]
 $\Sigma 2 = \text{Table}[\text{Total}[\text{Table}[Pm[[s2ordered[[i]]]] * \Delta v2[[s2ordered[[i]]]] * \delta^k[[i]]],
                \{i, 25, 1, -1\}], \{d, 0, 1, 0.01\}]$ 
ListPlot[ $\Sigma 2$ , DataRange -> {0, 1}, Filling -> Axis, AspectRatio -> 1 / 1,
         AxesLabel -> { $\delta$ , "Sum (9)"}, LabelStyle -> Directive[Black, Large]]

{{0, -200, -300, -450, -700}}
{{0, -166.66, -300, -450, -900}}
{{0.15, 0.3, 0.3, 0.2, 0.05}}
0.1
{{0., 0.9994, 0.999667, 0.999778, 0.999889},
 {0.9995, 0.0909041, 0.19996, 0.384556, 0.636306},
 {0.999667, 0.285671, 0., 0.199973, 0.499958},
 {0.999778, 0.459401, 0.199973, 0., 0.333309},
 {0.999857, 0.615326, 0.39996, 0.217372, 0.124992}}
{{0, 166.66, 300, 450, 900},
 {-200, -33.34, 100, 250, 700}, {-300, -133.34, 0, 150, 600},
 {-450, -283.34, -150, 0, 450}, {-700, -533.34, -400, -250, 200}}
```

A.1 Appendix: Experiment 1

2 | *Saliency calculations L8 VS L6 graph_FontLabel.nb*

```

***** This is the list of all (1) saliencies, (2)  $\Delta v$ 's and (3) probabilities:
{0., 0.9994, 0.999667, 0.999778, 0.999889, 0.9995, 0.0909041, 0.19996, 0.384556,
 0.636306, 0.999667, 0.285671, 0., 0.199973, 0.499958, 0.999778, 0.459401,
 0.199973, 0., 0.333309, 0.999857, 0.615326, 0.39996, 0.217372, 0.124992}

{0, 166.66, 300, 450, 900, -200, -33.34, 100, 250, 700, -300, -133.34, 0,
 150, 600, -450, -283.34, -150, 0, 450, -700, -533.34, -400, -250, 200}

{0.15, 0.3, 0.3, 0.2, 0.05, 0.3, 0.3, 0.3, 0.2, 0.05, 0.3, 0.3, 0.3,
 0.2, 0.05, 0.2, 0.2, 0.2, 0.2, 0.05, 0.05, 0.05, 0.05, 0.05, 0.05}

The most salient pair is :  $\sigma = 0.999889$ 

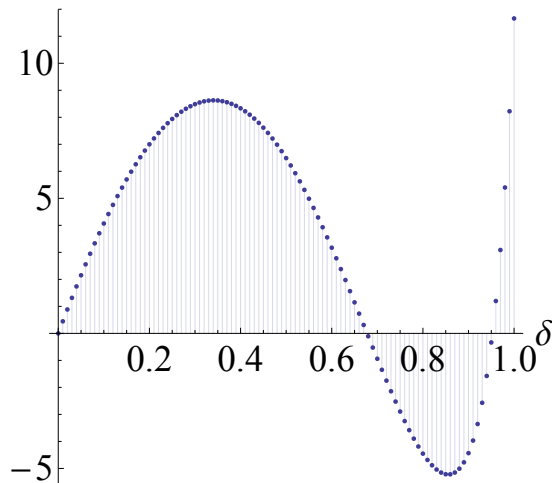
***** This is the ordering of
the saliency elements of table s2 (smallest to largest):
{1, 13, 19, 7, 25, 8, 14, 18, 24, 12,
 20, 9, 23, 17, 15, 22, 10, 2, 6, 3, 11, 4, 16, 21, 5}

{25, 24, 23, 22, 21, 20, 19, 18, 17, 16,
 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1}

Calculations for A=L10 and B=L11 for
a range of  $\delta$ 's (positive values imply that L10 > L11)
{0., 0.446411, 0.885294, 1.31614, 1.73846, 2.15179, 2.55566, 2.94965, 3.33333,
 3.70631, 4.06818, 4.41859, 4.75715, 5.08353, 5.3974, 5.69841, 5.98628,
 6.26068, 6.52135, 6.76799, 7.00034, 7.21814, 7.42115, 7.60913, 7.78185,
 7.93911, 8.08069, 8.20641, 8.31608, 8.40954, 8.48662, 8.54719, 8.5911,
 8.61824, 8.62852, 8.62183, 8.59812, 8.55732, 8.49941, 8.42436, 8.33219,
 8.22293, 8.09663, 7.95337, 7.79326, 7.61645, 7.42309, 7.21341, 6.98764,
 6.74606, 6.489, 6.21682, 5.92993, 5.62879, 5.31392, 4.98588, 4.64529,
 4.29283, 3.92924, 3.55533, 3.17196, 2.78008, 2.38069, 1.97488, 1.56379,
 1.14866, 0.730808, 0.311614, -0.107445, -0.52481, -0.93883, -1.34776,
 -1.74976, -2.14288, -2.52503, -2.89402, -3.24748, -3.58288, -3.89747,
 -4.18823, -4.45187, -4.68469, -4.88253, -5.04067, -5.15363, -5.2151,
 -5.21759, -5.15229, -5.00866, -4.77406, -4.43326, -3.96785, -3.35552,
 -2.56921, -1.57608, -0.336257, 1.19859, 3.08703, 5.39992, 8.22285, 11.659}

```

Sum (9)



A.1 Appendix: Experiment 1

A.1.12.4 Salience Calculations of L9 VS L10 with Graph

```
LotteryA = {{-45, -220, -300, -450, -900}}
LotteryB = {{-50, -170, -300, -400, -1000}}
P = {{0.85, 0.08, 0.035, 0.025, 0.01}}
 $\theta = 0.1$ 
 $\sigma[x_, y_] := (\text{Abs}[x - y]) / (\text{Abs}[x] + \text{Abs}[y] + \theta)$ 

(* calculate a table with all  $\sigma$ 's // N[] is for decimal numbers *)
s = Table[N[ $\sigma$ [LotteryA[[1, i]], LotteryB[[1, j]]]], {i, 1, 5}, {j, 1, 5}]
(* calculate a table with all plain outcome differences *)
 $\Delta v = \text{Table}[\text{LotteryA}[[1, i]] - \text{LotteryB}[[1, j]], \{i, 1, 5\}, \{j, 1, 5\}]$ 

Print["***** This is the list of
      all (1) saliences, (2)  $\Delta v$ 's and (3) probabilities: "]
s2 = Flatten[ArrayReshape[s, {1, 25}]]
 $\Delta v2 = \text{Flatten}[\text{ArrayReshape}[\Delta v, \{1, 25\}]]$ 
Pm = Flatten[List[P, {P[[1, 2]], P[[1, 2]], P[[1, 3]], P[[1, 4]], P[[1, 5]]}],
             {{P[[1, 3]], P[[1, 3]], P[[1, 3]], P[[1, 4]], P[[1, 5]]}},
             {{P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 5]]}},
             {{P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]]}}]
Print["The most salient pair is :  $\sigma =$ ", Max[s]]

Print["***** This is the ordering of the
      salience elements of table s2 (smallest to largest):"]
s2ordered = Ordering[s2]
k = Range[25, 1, -1]

(* with various  $\delta$ s ---
   can find  $\delta$  which is switching point of preference between Lottery A and B *)
Print["Calculations for A=L10 and B=L11 for a
      range of  $\delta$ 's (positive values imply that L10 > L11) "]
 $\Sigma 2 = \text{Table}[\text{Total}[\text{Table}[Pm[[s2ordered[[i]]]] * \Delta v2[[s2ordered[[i]]]] * d^k[[i]]],
                \{i, 25, 1, -1\}], \{d, 0, 1, 0.01\}]$ 
ListPlot[ $\Sigma 2$ , DataRange -> {0, 1}, Filling -> Axis, AspectRatio -> 1 / 1,
          AxesLabel -> { $\delta$ , "Sum (9)"}, LabelStyle -> Directive[Black, Large]]

{{-45, -220, -300, -450, -900}}
{{-50, -170, -300, -400, -1000}}
{{0.85, 0.08, 0.035, 0.025, 0.01}}
0.1
{{0.0525762, 0.581125, 0.738916, 0.797574, 0.913788},
 {0.629397, 0.128172, 0.153817, 0.290276, 0.639292},
 {0.714082, 0.276537, 0., 0.142837, 0.53842},
 {0.79984, 0.45154, 0.199973, 0.0588166, 0.379284},
 {0.894643, 0.682179, 0.499958, 0.384586, 0.0526288}}
{{5, 125, 255, 355, 955}, {-170, -50, 80, 180, 780}, {-250, -130, 0, 100, 700},
 {-400, -280, -150, -50, 550}, {-850, -730, -600, -500, 100}}
***** This is the list of all (1) saliences, (2)  $\Delta v$ 's and (3) probabilities:
```

A.1 Appendix: Experiment 1

2 | *Saliency calculations L9 VS L10 graph_FontLabel.nb*

```
{0.0525762, 0.581125, 0.738916, 0.797574, 0.913788, 0.629397, 0.128172, 0.153817,
 0.290276, 0.639292, 0.714082, 0.276537, 0., 0.142837, 0.53842, 0.79984, 0.45154,
 0.199973, 0.0588166, 0.379284, 0.894643, 0.682179, 0.499958, 0.384586, 0.0526288}

{5, 125, 255, 355, 955, -170, -50, 80, 180, 780, -250, -130, 0,
 100, 700, -400, -280, -150, -50, 550, -850, -730, -600, -500, 100}

{0.85, 0.08, 0.035, 0.025, 0.01, 0.08, 0.08, 0.035, 0.025, 0.01, 0.035, 0.035,
 0.035, 0.025, 0.01, 0.025, 0.025, 0.025, 0.025, 0.01, 0.01, 0.01, 0.01, 0.01}

The most salient pair is :  $\sigma = 0.913788$ 

***** This is the ordering of
the saliency elements of table s2 (smallest to largest):

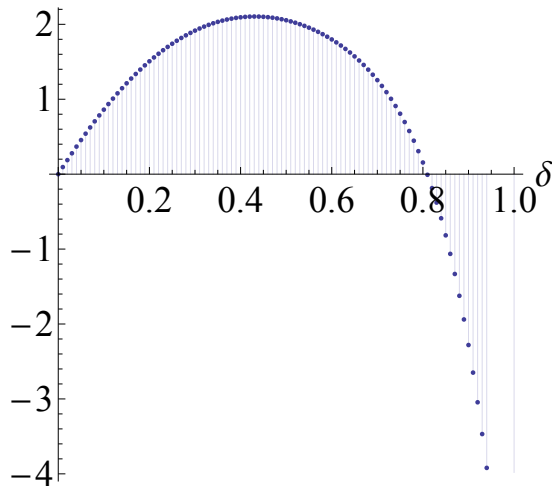
{13, 1, 25, 19, 7, 14, 8, 18, 12, 9, 20,
 24, 17, 23, 15, 2, 6, 10, 22, 11, 3, 4, 16, 21, 5}

{25, 24, 23, 22, 21, 20, 19, 18, 17, 16,
 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1}

Calculations for A=L10 and B=L11 for
a range of  $\delta$ 's (positive values imply that L10 > L11)

{0., 0.0946401, 0.187521, 0.278587, 0.367784, 0.455058, 0.540362, 0.623647,
 0.70487, 0.78399, 0.860967, 0.935766, 1.00835, 1.0787, 1.14678, 1.21256,
 1.27603, 1.33716, 1.39595, 1.45237, 1.50642, 1.55808, 1.60737, 1.65426,
 1.69876, 1.74088, 1.78062, 1.81798, 1.85297, 1.88561, 1.91591, 1.94388,
 1.96953, 1.99289, 2.01396, 2.03277, 2.04934, 2.06368, 2.07581, 2.08576,
 2.09353, 2.09914, 2.10262, 2.10397, 2.1032, 2.10033, 2.09536, 2.08829,
 2.07913, 2.06787, 2.0545, 2.03901, 2.02138, 2.00157, 1.97956, 1.95531,
 1.92876, 1.89985, 1.86851, 1.83466, 1.7982, 1.75901, 1.71697, 1.67193,
 1.62372, 1.57215, 1.51699, 1.45802, 1.39493, 1.32744, 1.25518, 1.17775,
 1.09472, 1.00559, 0.909808, 0.80675, 0.695731, 0.575987, 0.446673,
 0.306856, 0.155512, -0.00847786, -0.18633, -0.379357, -0.588962, -0.81663,
 -1.06391, -1.33239, -1.62365, -1.93924, -2.28057, -2.64881, -3.04479,
 -3.46883, -3.92047, -4.39823, -4.89924, -5.41877, -5.94964, -6.48152, -7.}
```

Sum (9)



A.1 Appendix: Experiment 1

A.1.12.5 Saliency Calculations of L4 VS L12 with Graph

```
LotteryA = {{-50, -150, -300, -450, -1000}}
LotteryB = {{-46, -180, -350, -480, -900}}
P = {{0.85, 0.08, 0.035, 0.025, 0.01}}
 $\theta = 0.1$ 
 $\sigma[x_, y_] := (\text{Abs}[x - y]) / (\text{Abs}[x] + \text{Abs}[y] + \theta)$ 

(* calculate a table with all  $\sigma$ 's // N[] is for decimal numbers *)
s = Table[N[ $\sigma$ [LotteryA[[1, i]], LotteryB[[1, j]]]], {i, 1, 5}, {j, 1, 5}]
(* calculate a table with all plain outcome differences *)
 $\Delta v$  = Table[LotteryA[[1, i]] - LotteryB[[1, j]], {i, 1, 5}, {j, 1, 5}]

Print["***** This is the list of
      all (1) saliencies, (2)  $\Delta v$ 's and (3) probabilities: "]
s2 = Flatten[ArrayReshape[s, {1, 25}]]
 $\Delta v2$  = Flatten[ArrayReshape[ $\Delta v$ , {1, 25}]]
Pm = Flatten[List[P, {P[[1, 2]], P[[1, 2]], P[[1, 3]], P[[1, 4]], P[[1, 5]]}],
            {{P[[1, 3]], P[[1, 3]], P[[1, 3]], P[[1, 4]], P[[1, 5]]},
            {{P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 4]], P[[1, 5]]},
            {{P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]], P[[1, 5]]}]]
Print["The most salient pair is :  $\sigma =$ ", Max[s]]

Print["***** This is the ordering of the
      saliency elements of table s2 (smallest to largest):"]
s2ordered = Ordering[s2]
k = Range[25, 1, -1]

(* with various  $\delta$ s ---
   can find  $\delta$  which is switching point of preference between Lottery A and B *)
Print["Calculations for A=L10 and B=L11 for a
      range of  $\delta$ 's (positive values imply that L10 > L11) "]
 $\Sigma 2$  = Table[Total[ Table[ Pm[[s2ordered[[i]]]] *  $\Delta v2$ [[s2ordered[[i]]]] * d^k[[i]],
            {i, 25, 1, -1} ] ] , {d, 0, 1, 0.01}]
ListPlot[ $\Sigma 2$ , DataRange -> {0, 1}, Filling -> Axis, AspectRatio -> 1 / 1,
          AxesLabel -> { $\delta$ , "Sum (9)"}, LabelStyle -> Directive[Black, Large]]

{{-50, -150, -300, -450, -1000}}
{{-46, -180, -350, -480, -900}}
{{0.85, 0.08, 0.035, 0.025, 0.01}}
0.1
{{0.0416233, 0.564972, 0.749813, 0.811168, 0.894643},
 {0.530342, 0.0908816, 0.39992, 0.523726, 0.714218},
 {0.733892, 0.249948, 0.0769112, 0.23074, 0.499958},
 {0.814352, 0.428503, 0.124984, 0.0322546, 0.333309},
 {0.911959, 0.694856, 0.481446, 0.351328, 0.0526288}}
{{-4, 130, 300, 430, 850}, {-104, 30, 200, 330, 750}, {-254, -120, 50, 180, 600},
 {-404, -270, -100, 30, 450}, {-954, -820, -650, -520, -100}}
***** This is the list of all (1) saliencies, (2)  $\Delta v$ 's and (3) probabilities:
```

A.1 Appendix: Experiment 1

2 | *Saliency calculations L4 VS L12 graph_FontLabel.nb*

```
{0.0416233, 0.564972, 0.749813, 0.811168, 0.894643, 0.530342,
 0.0908816, 0.39992, 0.523726, 0.714218, 0.733892, 0.249948,
 0.0769112, 0.23074, 0.499958, 0.814352, 0.428503, 0.124984, 0.0322546,
 0.333309, 0.911959, 0.694856, 0.481446, 0.351328, 0.0526288}

{-4, 130, 300, 430, 850, -104, 30, 200, 330, 750, -254, -120, 50,
 180, 600, -404, -270, -100, 30, 450, -954, -820, -650, -520, -100}

{0.85, 0.08, 0.035, 0.025, 0.01, 0.08, 0.08, 0.035, 0.025, 0.01, 0.035, 0.035,
 0.035, 0.025, 0.01, 0.025, 0.025, 0.025, 0.025, 0.01, 0.01, 0.01, 0.01, 0.01, 0.01}

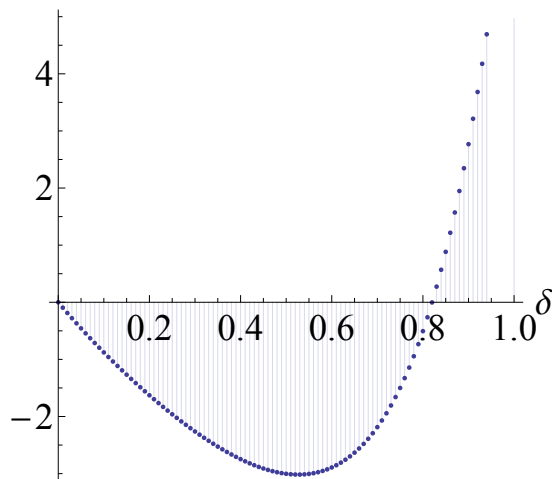
The most salient pair is :  $\sigma = 0.911959$ 

***** This is the ordering of
the saliency elements of table s2 (smallest to largest):
{19, 1, 25, 13, 7, 18, 14, 12, 20, 24,
 8, 17, 23, 15, 9, 6, 2, 22, 10, 11, 3, 4, 16, 5, 21}

{25, 24, 23, 22, 21, 20, 19, 18, 17, 16,
 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1}

Calculations for A=L10 and B=L11 for
a range of  $\delta$ 's (positive values imply that L10 > L11)
{0., -0.09456, -0.187479, -0.278814, -0.368618, -0.456942, -0.543835, -0.62934,
-0.713499, -0.79635, -0.877928, -0.958265, -1.03739, -1.11532, -1.19208,
-1.26769, -1.34216, -1.41549, -1.4877, -1.55878, -1.62873, -1.69754,
-1.76521, -1.8317, -1.89702, -1.96112, -2.02398, -2.08558, -2.14586,
-2.20479, -2.26232, -2.3184, -2.37297, -2.42597, -2.47734, -2.52701,
-2.57489, -2.62091, -2.66499, -2.70703, -2.74693, -2.7846, -2.81993,
-2.85279, -2.88308, -2.91067, -2.93543, -2.9572, -2.97587, -2.99125,
-3.00321, -3.01156, -3.01614, -3.01675, -3.0132, -3.00529, -2.9928,
-2.97551, -2.95317, -2.92554, -2.89236, -2.85335, -2.80821, -2.75666,
-2.69835, -2.63295, -2.56011, -2.47945, -2.39057, -2.29305, -2.18645,
-2.07032, -1.94415, -1.80744, -1.65963, -1.50017, -1.32845, -1.14383,
-0.945663, -0.733245, -0.505853, -0.262732, -0.00309432, 0.27387,
0.568994, 0.883128, 1.21712, 1.57183, 1.94806, 2.3466, 2.76812, 3.2132,
3.6822, 4.17526, 4.69216, 5.23221, 5.79409, 6.37571, 6.97387, 7.58406, 8.2}
```

Sum (9)



A.1 Appendix: Experiment 1

A.1.13 SPSS Syntax Code

The following code includes data cleaning and analysis in SPSS version 21 [1].

```
1  *USE ALL.
2  ***** DATA CLEANING *****.
3  RECODE S1 (2=0) (1=1).
4  RECODE YourTotalDuration (CONVERT) INTO DURATION.
5  ***** Survey *****
6  ** fixing coding of AGE **.
7  COMPUTE S18=S18_1 + 18.
8  ** recode Number of Dependents: 7 is 0 **.
9  RECODE S22_1 (7=0).
10 VARIABLE LABELS S22_1 'Family dep.'.
11 ** recodde Income to exclude 'prefer not to answer' from Scatterplots **.
12 RECODE S17_1 (12=SYSMIS) INTO S17.
13 ** change LABELS (for fit in Scatterplots) **.
14 VARIABLE LABELS S5_1 'Risk'.
15 VARIABLE LABELS S18 'Age'.
16 VARIABLE LABELS S21 'Marital Status'.
17 VARIABLE LABELS S19 'Gender'.
18 VARIABLE LABELS S20_1 'Education'.
19 VARIABLE LABELS S2_1 'Yrs of Exp'.
20 VARIABLE LABELS S3_1 'Current Job'.
21 VARIABLE LABELS S4 'Incident Exp'.
22 VARIABLE LABELS S8_1 'Sec-Ops @work'.
23 VARIABLE LABELS S9_1 'Sec-bus @work'.
24 VARIABLE LABELS S10_1 'Sec-bus general'.
25 VARIABLE LABELS S11_1 'Sacr Sec4Speed'.
26 VARIABLE LABELS S12 'Job Title'.
27 VARIABLE LABELS S13 'Indep. Decisions'.
28 VARIABLE LABELS S14 'More CIA'.
29 VARIABLE LABELS S15 'Who makes decisions'.
30 VARIABLE LABELS S17_1 'Income'.
31 ** create PROFESSIONAL var from STUDENT var for MODERATION in Regressions **.
32 RECODE STUDENT (0=1) (1=0) INTO PROFESSIONAL.
33
34 ***** HYPOTHESIS 3 (H3) ***** Fill in empty fields of H3 and create the variable=H3Group for the Non-
    Parametric tests.
35 RECODE H3 (MISSING=2).
36 RECODE H3 (1=1) (2=2) INTO H3Group.
37 VARIABLE LABELS H3Group 'Was H3 presented?'.
38 VALUE LABELS H3Group
39 1 'H3'
40 2 'no H3'.
41
42 RECODE H5_1A_9_10_1_1 (MISSING=0).
43 RECODE H5_1A_8_10_1_1 (MISSING=0).
44 RECODE H5_1A_7_10_1_1 (MISSING=0).
45 RECODE H5_1A_6_10_1_1 (MISSING=0).
46 RECODE H5_1A_5_10_1_1 (MISSING=0).
47 RECODE H5_1A_4_10_1_1 (MISSING=0).
48 RECODE H5_1A_3_10_1_1 (MISSING=0).
49 RECODE H5_1A_2_10_1_1 (MISSING=0).
50 RECODE H5_1A_1_10_1_1 (MISSING=0).
51
52 RECODE H5_1B_10_9_1_1 (MISSING=0).
```

A.1 Appendix: Experiment 1

```
53 RECODE H5_1B_10_8_1_1 (MISSING=0).
54 RECODE H5_1B_10_7_1_1 (MISSING=0).
55 RECODE H5_1B_10_6_1_1 (MISSING=0).
56 RECODE H5_1B_10_5_1_1 (MISSING=0).
57 RECODE H5_1B_10_4_1_1 (MISSING=0).
58 RECODE H5_1B_10_3_1_1 (MISSING=0).
59 RECODE H5_1B_10_2_1_1 (MISSING=0).
60 RECODE H5_1B_10_1_1_1 (MISSING=0).
61
62 ***** How to create a single FLAG-variable = RISK_FIRST (0 or 1) from RiskToAmbiguity variable for the Non-
        Parametric tests:.
63 RECODE RiskToAmbiguity (CONVERT) INTO RISK_FIRST.
64 RECODE RISK_FIRST (1=1) (MISSING=0).
65 VARIABLE LABELS RISK_FIRST 'Was Risk presented first in H1?'.
66 VALUE LABELS RISK_FIRST
67 1 'Risk to Ambiguity'
68 0 'Ambiguity to Risk'.
69 EXECUTE.
70 *Consolidate all H1 data (RISK_FIRST or not) into one set of 12 vars.
71 DO IF (RISK_FIRST = 1).
72 COMPUTE H1_1 = H1_1_1.
73 COMPUTE H1_2 = H1_2_1.
74 COMPUTE H1_3 = H1_3_1.
75 COMPUTE H1_4 = H1_4_1.
76 COMPUTE H1_5 = H1_5_1.
77 COMPUTE H1_6 = H1_6_1.
78 COMPUTE H1_7 = H1_7_1.
79 COMPUTE H1_8 = H1_8_1.
80 COMPUTE H1_9 = H1_9_1.
81 COMPUTE H1_10 = H1_10_1.
82 COMPUTE H1_11 = H1_11_1.
83 COMPUTE H1_12 = H1_12_1.
84 ELSE IF (RISK_FIRST = 0).
85 COMPUTE H1_1 = H1_1ar_1.
86 COMPUTE H1_2 = H1_2ar_1.
87 COMPUTE H1_3 = H1_3ar_1.
88 COMPUTE H1_4 = H1_4ar_1.
89 COMPUTE H1_5 = H1_5ar_1.
90 COMPUTE H1_6 = H1_6ar_1.
91 COMPUTE H1_7 = H1_7ar_1.
92 COMPUTE H1_8 = H1_8ar_1.
93 COMPUTE H1_9 = H1_9ar_1.
94 COMPUTE H1_10 = H1_10ar_1.
95 COMPUTE H1_11 = H1_11ar_1.
96 COMPUTE H1_12 = H1_12ar_1.
97 END IF.
98 VARIABLE LEVEL H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 (SCALE).
99
100 ***** H1_i and H2_6,7,8: New variables with the distance from the Expected Values (Risk Aversion).
101 * First I define the Expected Values for the H1_i series.
102 COMPUTE EV_H1_1to4 = 2.5.
103 COMPUTE EV_H1_5to8 = 7.5.
104 COMPUTE EV_H1_9to12 = 25.
105 * And the distances for the H2 series WTP questions (H2_6.1 H2_7.1 H2_8.1).
106 COMPUTE EV_H2_6 = 86.6.
107 COMPUTE EV_H2_7 = 86.6.
108 COMPUTE EV_H2_8 = 89.75.
```

A.1 Appendix: Experiment 1

```
109 * Then I calculate the distance of each variable from the Expected Value (so that I can compare the distances).
110 COMPUTE RiskAversionH1_1 = H1_1 - EV_H1_1to4.
111 COMPUTE RiskAversionH1_2 = H1_2 - EV_H1_1to4.
112 COMPUTE RiskAversionH1_3 = H1_3 - EV_H1_1to4.
113 COMPUTE RiskAversionH1_4 = H1_4 - EV_H1_1to4.
114 COMPUTE RiskAversionH1_5 = H1_5 - EV_H1_5to8.
115 COMPUTE RiskAversionH1_6 = H1_6 - EV_H1_5to8.
116 COMPUTE RiskAversionH1_7 = H1_7 - EV_H1_5to8.
117 COMPUTE RiskAversionH1_8 = H1_8 - EV_H1_5to8.
118 COMPUTE RiskAversionH1_9 = H1_9 - EV_H1_9to12.
119 COMPUTE RiskAversionH1_10 = H1_10 - EV_H1_9to12.
120 COMPUTE RiskAversionH1_11 = H1_11 - EV_H1_9to12.
121 COMPUTE RiskAversionH1_12 = H1_12 - EV_H1_9to12.
122 COMPUTE RiskAversionH2_6 = H2_6.1 - EV_H2_6.
123 COMPUTE RiskAversionH2_7 = H2_7.1 - EV_H2_7.
124 COMPUTE RiskAversionH2_8 = H2_8.1 - EV_H2_8.
125 * Then I calculate the distance as a percentage of each Expected Value (so that I can compare the distances
    across all risky lotteries, across all ambiguous etc.).
126 COMPUTE RiskAversionH1_1ratio = RiskAversionH1_1/EV_H1_1to4.
127 COMPUTE RiskAversionH1_2ratio = RiskAversionH1_2/EV_H1_1to4.
128 COMPUTE RiskAversionH1_3ratio = RiskAversionH1_3/EV_H1_1to4.
129 COMPUTE RiskAversionH1_4ratio = RiskAversionH1_4/EV_H1_1to4.
130 COMPUTE RiskAversionH1_5ratio = RiskAversionH1_5/EV_H1_5to8.
131 COMPUTE RiskAversionH1_6ratio = RiskAversionH1_6/EV_H1_5to8.
132 COMPUTE RiskAversionH1_7ratio = RiskAversionH1_7/EV_H1_5to8.
133 COMPUTE RiskAversionH1_8ratio = RiskAversionH1_8/EV_H1_5to8.
134 COMPUTE RiskAversionH1_9ratio = RiskAversionH1_9/EV_H1_9to12.
135 COMPUTE RiskAversionH1_10ratio = RiskAversionH1_10/EV_H1_9to12.
136 COMPUTE RiskAversionH1_11ratio = RiskAversionH1_11/EV_H1_9to12.
137 COMPUTE RiskAversionH1_12ratio = RiskAversionH1_12/EV_H1_9to12.
138 COMPUTE RiskAversionH2_6ratio = RiskAversionH2_6/EV_H2_6.
139 COMPUTE RiskAversionH2_7ratio = RiskAversionH2_7/EV_H2_7.
140 COMPUTE RiskAversionH2_8ratio = RiskAversionH2_8/EV_H2_8.
141
142 *** Finding the Switching Point for Hypothesis 4.
143 DO IF (H5_1A_1_1=1).
144     DO IF (H5_1A_9_10_1_1=2).
145         COMPUTE SWITCHPOINT_SEC=9.
146     END IF.
147     DO IF (H5_1A_8_10_1_1=2).
148         COMPUTE SWITCHPOINT_SEC=8.
149     END IF.
150     DO IF (H5_1A_7_10_1_1=2).
151         COMPUTE SWITCHPOINT_SEC=7.
152     END IF.
153     DO IF (H5_1A_6_10_1_1=2).
154         COMPUTE SWITCHPOINT_SEC=6.
155     END IF.
156     DO IF (H5_1A_5_10_1_1=2).
157         COMPUTE SWITCHPOINT_SEC=5.
158     END IF.
159     DO IF (H5_1A_4_10_1_1=2).
160         COMPUTE SWITCHPOINT_SEC=4.
161     END IF.
162     DO IF (H5_1A_3_10_1_1=2).
163         COMPUTE SWITCHPOINT_SEC=3.
164     END IF.
```

A.1 Appendix: Experiment 1

```
165 DO IF (H5_1A_2_10_1.1=2).
166     COMPUTE SWITCHPOINT_SEC=2.
167 END IF.
168 DO IF (H5_1A_1_10_1.1=2).
169     COMPUTE SWITCHPOINT_SEC=1.
170 ELSE IF (H5_1A_1_10_1.1=1).
171     COMPUTE SWITCHPOINT_SEC=0.
172 END IF.
173 ELSE IF (H5_1_1.1=2).
174     DO IF (H5_1B_10_9_1.1=2).
175         COMPUTE SWITCHPOINT_OPS=9.
176     END IF.
177     DO IF (H5_1B_10_8_1.1=2).
178         COMPUTE SWITCHPOINT_OPS=8.
179     END IF.
180     DO IF (H5_1B_10_7_1.1=2).
181         COMPUTE SWITCHPOINT_OPS=7.
182     END IF.
183     DO IF (H5_1B_10_6_1.1=2).
184         COMPUTE SWITCHPOINT_OPS=6.
185     END IF.
186     DO IF (H5_1B_10_5_1.1=2).
187         COMPUTE SWITCHPOINT_OPS=5.
188     END IF.
189     DO IF (H5_1B_10_4_1.1=2).
190         COMPUTE SWITCHPOINT_OPS=4.
191     END IF.
192     DO IF (H5_1B_10_3_1.1=2).
193         COMPUTE SWITCHPOINT_OPS=3.
194     END IF.
195     DO IF (H5_1B_10_2_1.1=2).
196         COMPUTE SWITCHPOINT_OPS=2.
197     END IF.
198     DO IF (H5_1B_10_1_1.1=2).
199         COMPUTE SWITCHPOINT_OPS=1.
200     ELSE IF (H5_1B_10_1_1.1=1).
201         COMPUTE SWITCHPOINT_OPS=0.
202     END IF.
203 END IF.
204
205 *Specifying the relative loss aversion only for the series H5_2x, for Hypothesis 4.
206 DO IF (H5_1_1.1=1).
207     DO IF (H5_2A_9_10_1.1=2 OR H5_2A_9_10_1.1=3).
208         COMPUTE LOSS_AV_SEC=0.
209     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_8_10_1.1=2 OR H5_3A_8_10_1.1=3)).
210         COMPUTE LOSS_AV_SEC=1.
211     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_7_10_1.1=2 OR H5_3A_7_10_1.1=3)).
212         COMPUTE LOSS_AV_SEC=2.
213     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_6_10_1.1=2 OR H5_3A_6_10_1.1=3)).
214         COMPUTE LOSS_AV_SEC=3.
215     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_5_10_1.1=2 OR H5_3A_5_10_1.1=3)).
216         COMPUTE LOSS_AV_SEC=4.
217     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_4_10_1.1=2 OR H5_3A_4_10_1.1=3)).
218         COMPUTE LOSS_AV_SEC=5.
219     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_3_10_1.1=2 OR H5_3A_3_10_1.1=3)).
220         COMPUTE LOSS_AV_SEC=6.
221     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_2_10_1.1=2 OR H5_3A_2_10_1.1=3)).
```

A.1 Appendix: Experiment 1

```
222     COMPUTE LOSS_AV_SEC=7.
223     ELSE IF (H5_2A_9_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
224         COMPUTE LOSS_AV_SEC=8.
225     ELSE IF (H5_2A_9_10_1.1=1 AND H5_3A_1_10_1.1=1).
226         COMPUTE LOSS_AV_SEC=9.
227     END IF.
228
229 DO IF (H5_2A_8_10_1.1=2 OR H5_2A_8_10_1.1=3).
230     COMPUTE LOSS_AV_SEC=0.
231     ELSE IF (H5_2A_8_10_1.1=1 AND (H5_3A_7_10_1.1=2 OR H5_3A_7_10_1.1=3)).
232         COMPUTE LOSS_AV_SEC=1.
233     ELSE IF (H5_2A_8_10_1.1=1 AND (H5_3A_6_10_1.1=2 OR H5_3A_6_10_1.1=3)).
234         COMPUTE LOSS_AV_SEC=2.
235     ELSE IF (H5_2A_8_10_1.1=1 AND (H5_3A_5_10_1.1=2 OR H5_3A_5_10_1.1=3)).
236         COMPUTE LOSS_AV_SEC=3.
237     ELSE IF (H5_2A_8_10_1.1=1 AND (H5_3A_4_10_1.1=2 OR H5_3A_4_10_1.1=3)).
238         COMPUTE LOSS_AV_SEC=4.
239     ELSE IF (H5_2A_8_10_1.1=1 AND (H5_3A_3_10_1.1=2 OR H5_3A_3_10_1.1=3)).
240         COMPUTE LOSS_AV_SEC=5.
241     ELSE IF (H5_2A_8_10_1.1=1 AND (H5_3A_2_10_1.1=2 OR H5_3A_2_10_1.1=3)).
242         COMPUTE LOSS_AV_SEC=6.
243     ELSE IF (H5_2A_8_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
244         COMPUTE LOSS_AV_SEC=7.
245     ELSE IF (H5_2A_8_10_1.1=1 AND H5_3A_1_10_1.1=1).
246         COMPUTE LOSS_AV_SEC=8.
247     END IF.
248
249 DO IF (H5_2A_7_10_1.1=2 OR H5_2A_7_10_1.1=3).
250     COMPUTE LOSS_AV_SEC=0.
251     ELSE IF (H5_2A_7_10_1.1=1 AND (H5_3A_6_10_1.1=2 OR H5_3A_6_10_1.1=3)).
252         COMPUTE LOSS_AV_SEC=1.
253     ELSE IF (H5_2A_7_10_1.1=1 AND (H5_3A_5_10_1.1=2 OR H5_3A_5_10_1.1=3)).
254         COMPUTE LOSS_AV_SEC=2.
255     ELSE IF (H5_2A_7_10_1.1=1 AND (H5_3A_4_10_1.1=2 OR H5_3A_4_10_1.1=3)).
256         COMPUTE LOSS_AV_SEC=3.
257     ELSE IF (H5_2A_7_10_1.1=1 AND (H5_3A_3_10_1.1=2 OR H5_3A_3_10_1.1=3)).
258         COMPUTE LOSS_AV_SEC=4.
259     ELSE IF (H5_2A_7_10_1.1=1 AND (H5_3A_2_10_1.1=2 OR H5_3A_2_10_1.1=3)).
260         COMPUTE LOSS_AV_SEC=5.
261     ELSE IF (H5_2A_7_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
262         COMPUTE LOSS_AV_SEC=6.
263     ELSE IF (H5_2A_7_10_1.1=1 AND H5_3A_1_10_1.1=1).
264         COMPUTE LOSS_AV_SEC=7.
265     END IF.
266
267 DO IF (H5_2A_6_10_1.1=2 OR H5_2A_6_10_1.1=3).
268     COMPUTE LOSS_AV_SEC=0.
269     ELSE IF (H5_2A_6_10_1.1=1 AND (H5_3A_5_10_1.1=2 OR H5_3A_5_10_1.1=3)).
270         COMPUTE LOSS_AV_SEC=1.
271     ELSE IF (H5_2A_6_10_1.1=1 AND (H5_3A_4_10_1.1=2 OR H5_3A_4_10_1.1=3)).
272         COMPUTE LOSS_AV_SEC=2.
273     ELSE IF (H5_2A_6_10_1.1=1 AND (H5_3A_3_10_1.1=2 OR H5_3A_3_10_1.1=3)).
274         COMPUTE LOSS_AV_SEC=3.
275     ELSE IF (H5_2A_6_10_1.1=1 AND (H5_3A_2_10_1.1=2 OR H5_3A_2_10_1.1=3)).
276         COMPUTE LOSS_AV_SEC=4.
277     ELSE IF (H5_2A_6_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
278         COMPUTE LOSS_AV_SEC=5.
```

A.1 Appendix: Experiment 1

```
279 ELSE IF (H5_2A_6_10_1.1=1 AND H5_3A_1_10_1.1=1).
280     COMPUTE LOSS_AV_SEC=6.
281 END IF.
282
283 DO IF (H5_2A_5_10_1.1=2 OR H5_2A_5_10_1.1=3).
284     COMPUTE LOSS_AV_SEC=0.
285 ELSE IF (H5_2A_5_10_1.1=1 AND (H5_3A_4_10_1.1=2 OR H5_3A_4_10_1.1=3)).
286     COMPUTE LOSS_AV_SEC=1.
287 ELSE IF (H5_2A_5_10_1.1=1 AND (H5_3A_3_10_1.1=2 OR H5_3A_3_10_1.1=3)).
288     COMPUTE LOSS_AV_SEC=2.
289 ELSE IF (H5_2A_5_10_1.1=1 AND (H5_3A_2_10_1.1=2 OR H5_3A_2_10_1.1=3)).
290     COMPUTE LOSS_AV_SEC=3.
291 ELSE IF (H5_2A_5_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
292     COMPUTE LOSS_AV_SEC=4.
293 ELSE IF (H5_2A_5_10_1.1=1 AND H5_3A_1_10_1.1=1).
294     COMPUTE LOSS_AV_SEC=5.
295 END IF.
296
297 DO IF (H5_2A_4_10_1.1=2 OR H5_2A_4_10_1.1=3).
298     COMPUTE LOSS_AV_SEC=0.
299 ELSE IF (H5_2A_4_10_1.1=1 AND (H5_3A_3_10_1.1=2 OR H5_3A_3_10_1.1=3)).
300     COMPUTE LOSS_AV_SEC=1.
301 ELSE IF (H5_2A_5_10_1.1=1 AND (H5_3A_2_10_1.1=2 OR H5_3A_2_10_1.1=3)).
302     COMPUTE LOSS_AV_SEC=3.
303 ELSE IF (H5_2A_5_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
304     COMPUTE LOSS_AV_SEC=4.
305 ELSE IF (H5_2A_5_10_1.1=1 AND H5_3A_1_10_1.1=1).
306     COMPUTE LOSS_AV_SEC=5.
307 END IF.
308
309 DO IF (H5_2A_3_10_1.1=2 OR H5_2A_3_10_1.1=3).
310     COMPUTE LOSS_AV_SEC=0.
311 ELSE IF (H5_2A_3_10_1.1=1 AND (H5_3A_2_10_1.1=2 OR H5_3A_2_10_1.1=3)).
312     COMPUTE LOSS_AV_SEC=1.
313 ELSE IF (H5_2A_3_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
314     COMPUTE LOSS_AV_SEC=2.
315 ELSE IF (H5_2A_3_10_1.1=1 AND H5_3A_1_10_1.1=1).
316     COMPUTE LOSS_AV_SEC=3.
317 END IF.
318
319 DO IF (H5_2A_2_10_1.1=2 OR H5_2A_2_10_1.1=3).
320     COMPUTE LOSS_AV_SEC=0.
321 ELSE IF (H5_2A_2_10_1.1=1 AND (H5_3A_1_10_1.1=2 OR H5_3A_1_10_1.1=3)).
322     COMPUTE LOSS_AV_SEC=1.
323 ELSE IF (H5_2A_2_10_1.1=1 AND H5_3A_1_10_1.1=1).
324     COMPUTE LOSS_AV_SEC=2.
325 END IF.
326
327 DO IF (H5_2A_1_10_1.1=2 OR H5_2A_1_10_1.1=3).
328     COMPUTE LOSS_AV_SEC=0.
329 ELSE IF (H5_2A_1_10_1.1=1).
330     COMPUTE LOSS_AV_SEC=1.
331 END IF.
332
333 ELSE IF (H5_1_1.1=2).
334     DO IF (H5_2B_10_9_1.1=2 OR H5_2B_10_9_1.1=3).
335         COMPUTE LOSS_AV_OPS=0.
```

A.1 Appendix: Experiment 1

```
336 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.8.1.1=2 OR H5_3B_10.8.1.1=3)).
337     COMPUTE LOSS_AV_OPS=1.
338 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.7.1.1=2 OR H5_3B_10.7.1.1=3)).
339     COMPUTE LOSS_AV_OPS=2.
340 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.6.1.1=2 OR H5_3B_10.6.1.1=3)).
341     COMPUTE LOSS_AV_OPS=3.
342 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.5.1.1=2 OR H5_3B_10.5.1.1=3)).
343     COMPUTE LOSS_AV_OPS=4.
344 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.4.1.1=2 OR H5_3B_10.4.1.1=3)).
345     COMPUTE LOSS_AV_OPS=5.
346 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.3.1.1=2 OR H5_3B_10.3.1.1=3)).
347     COMPUTE LOSS_AV_OPS=6.
348 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.2.1.1=2 OR H5_3B_10.2.1.1=3)).
349     COMPUTE LOSS_AV_OPS=7.
350 ELSE IF (H5_2B_10.9.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
351     COMPUTE LOSS_AV_OPS=8.
352 ELSE IF (H5_2B_10.9.1.1=1 AND H5_3B_10.1.1.1=1).
353     COMPUTE LOSS_AV_OPS=9.
354 END IF.
355
356 DO IF (H5_2B_10.8.1.1=2 OR H5_2B_10.8.1.1=3).
357     COMPUTE LOSS_AV_OPS=0.
358 ELSE IF (H5_2B_10.8.1.1=1 AND (H5_3B_10.7.1.1=2 OR H5_3B_10.7.1.1=3)).
359     COMPUTE LOSS_AV_OPS=1.
360 ELSE IF (H5_2B_10.8.1.1=1 AND (H5_3B_10.6.1.1=2 OR H5_3B_10.6.1.1=3)).
361     COMPUTE LOSS_AV_OPS=2.
362 ELSE IF (H5_2B_10.8.1.1=1 AND (H5_3B_10.5.1.1=2 OR H5_3B_10.5.1.1=3)).
363     COMPUTE LOSS_AV_OPS=3.
364 ELSE IF (H5_2B_10.8.1.1=1 AND (H5_3B_10.4.1.1=2 OR H5_3B_10.4.1.1=3)).
365     COMPUTE LOSS_AV_OPS=4.
366 ELSE IF (H5_2B_10.8.1.1=1 AND (H5_3B_10.3.1.1=2 OR H5_3B_10.3.1.1=3)).
367     COMPUTE LOSS_AV_OPS=5.
368 ELSE IF (H5_2B_10.8.1.1=1 AND (H5_3B_10.2.1.1=2 OR H5_3B_10.2.1.1=3)).
369     COMPUTE LOSS_AV_OPS=6.
370 ELSE IF (H5_2B_10.8.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
371     COMPUTE LOSS_AV_OPS=7.
372 ELSE IF (H5_2B_10.8.1.1=1 AND H5_3B_10.1.1.1=1).
373     COMPUTE LOSS_AV_OPS=8.
374 END IF.
375
376 DO IF (H5_2B_10.7.1.1=2 OR H5_2B_10.7.1.1=3).
377     COMPUTE LOSS_AV_OPS=0.
378 ELSE IF (H5_2B_10.7.1.1=1 AND (H5_3B_10.6.1.1=2 OR H5_3B_10.6.1.1=3)).
379     COMPUTE LOSS_AV_OPS=1.
380 ELSE IF (H5_2B_10.7.1.1=1 AND (H5_3B_10.5.1.1=2 OR H5_3B_10.5.1.1=3)).
381     COMPUTE LOSS_AV_OPS=2.
382 ELSE IF (H5_2B_10.7.1.1=1 AND (H5_3B_10.4.1.1=2 OR H5_3B_10.4.1.1=3)).
383     COMPUTE LOSS_AV_OPS=3.
384 ELSE IF (H5_2B_10.7.1.1=1 AND (H5_3B_10.3.1.1=2 OR H5_3B_10.3.1.1=3)).
385     COMPUTE LOSS_AV_OPS=4.
386 ELSE IF (H5_2B_10.7.1.1=1 AND (H5_3B_10.2.1.1=2 OR H5_3B_10.2.1.1=3)).
387     COMPUTE LOSS_AV_OPS=5.
388 ELSE IF (H5_2B_10.7.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
389     COMPUTE LOSS_AV_OPS=6.
390 ELSE IF (H5_2B_10.7.1.1=1 AND H5_3B_10.1.1.1=1).
391     COMPUTE LOSS_AV_OPS=7.
392 END IF.
```

A.1 Appendix: Experiment 1

```
393
394 DO IF (H5_2B_10.6.1.1=2 OR H5_2B_10.6.1.1=3).
395     COMPUTE LOSS_AV_OPS=0.
396 ELSE IF (H5_2B_10.6.1.1=1 AND (H5_3B_10.5.1.1=2 OR H5_3B_10.5.1.1=3)).
397     COMPUTE LOSS_AV_OPS=1.
398 ELSE IF (H5_2B_10.6.1.1=1 AND (H5_3B_10.4.1.1=2 OR H5_3B_10.4.1.1=3)).
399     COMPUTE LOSS_AV_OPS=2.
400 ELSE IF (H5_2B_10.6.1.1=1 AND (H5_3B_10.3.1.1=2 OR H5_3B_10.3.1.1=3)).
401     COMPUTE LOSS_AV_OPS=3.
402 ELSE IF (H5_2B_10.6.1.1=1 AND (H5_3B_10.2.1.1=2 OR H5_3B_10.2.1.1=3)).
403     COMPUTE LOSS_AV_OPS=4.
404 ELSE IF (H5_2B_10.6.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
405     COMPUTE LOSS_AV_OPS=5.
406 ELSE IF (H5_2B_10.6.1.1=1 AND H5_3B_10.1.1.1=1).
407     COMPUTE LOSS_AV_OPS=6.
408 END IF.
409
410 DO IF (H5_2B_10.5.1.1=2 OR H5_2B_10.5.1.1=3).
411     COMPUTE LOSS_AV_OPS=0.
412 ELSE IF (H5_2B_10.5.1.1=1 AND (H5_3B_10.4.1.1=2 OR H5_3B_10.4.1.1=3)).
413     COMPUTE LOSS_AV_OPS=1.
414 ELSE IF (H5_2B_10.5.1.1=1 AND (H5_3B_10.3.1.1=2 OR H5_3B_10.3.1.1=3)).
415     COMPUTE LOSS_AV_OPS=2.
416 ELSE IF (H5_2B_10.5.1.1=1 AND (H5_3B_10.2.1.1=2 OR H5_3B_10.2.1.1=3)).
417     COMPUTE LOSS_AV_OPS=3.
418 ELSE IF (H5_2B_10.5.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
419     COMPUTE LOSS_AV_OPS=4.
420 ELSE IF (H5_2B_10.5.1.1=1 AND H5_3B_10.1.1.1=1).
421     COMPUTE LOSS_AV_OPS=5.
422 END IF.
423
424 DO IF (H5_2B_10.4.1.1=2 OR H5_2B_10.4.1.1=3).
425     COMPUTE LOSS_AV_OPS=0.
426 ELSE IF (H5_2B_10.4.1.1=1 AND (H5_3B_10.3.1.1=2 OR H5_3B_10.3.1.1=3)).
427     COMPUTE LOSS_AV_OPS=1.
428 ELSE IF (H5_2B_10.4.1.1=1 AND (H5_3B_10.2.1.1=2 OR H5_3B_10.2.1.1=3)).
429     COMPUTE LOSS_AV_OPS=2.
430 ELSE IF (H5_2B_10.4.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
431     COMPUTE LOSS_AV_OPS=3.
432 ELSE IF (H5_2B_10.4.1.1=1 AND H5_3B_10.1.1.1=1).
433     COMPUTE LOSS_AV_OPS=4.
434 END IF.
435
436 DO IF (H5_2B_10.3.1.1=2 OR H5_2B_10.3.1.1=3).
437     COMPUTE LOSS_AV_OPS=0.
438 ELSE IF (H5_2B_10.3.1.1=1 AND (H5_3B_10.2.1.1=2 OR H5_3B_10.2.1.1=3)).
439     COMPUTE LOSS_AV_OPS=1.
440 ELSE IF (H5_2B_10.3.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
441     COMPUTE LOSS_AV_OPS=2.
442 ELSE IF (H5_2B_10.3.1.1=1 AND H5_3B_10.1.1.1=1).
443     COMPUTE LOSS_AV_OPS=3.
444 END IF.
445
446 DO IF (H5_2B_10.2.1.1=2 OR H5_2B_10.2.1.1=3).
447     COMPUTE LOSS_AV_OPS=0.
448 ELSE IF (H5_2B_10.2.1.1=1 AND (H5_3B_10.1.1.1=2 OR H5_3B_10.1.1.1=3)).
449     COMPUTE LOSS_AV_OPS=1.
```


A.1 Appendix: Experiment 1

```
450 ELSE IF (H5_2B_10_2_1_1=1 AND H5_3B_10_1_1_1=1).
451     COMPUTE LOSS_AV_OPS=2.
452 END IF.
453
454 DO IF (H5_2B_10_1_1_1=2 OR H5_2B_10_1_1_1=3).
455     COMPUTE LOSS_AV_OPS=0.
456 ELSE IF (H5_2B_10_1_1_1=1).
457     COMPUTE LOSS_AV_OPS=1.
458 END IF.
459
460 END IF.
461
462 **** Use SWITCHPOINTS and LOSS_AVs for NP tests by H3_Group ****.
463 COMPUTE SWITCHPOINT_SEC_NUM = SWITCHPOINT_SEC.
464 RECODE SWITCHPOINT_SEC_NUM (SYSMIS=SYSMIS).
465 COMPUTE SWITCHPOINT_OPS_NUM = SWITCHPOINT_OPS.
466 RECODE SWITCHPOINT_OPS_NUM (SYSMIS=SYSMIS).
467
468 COMPUTE LOSS_AV_SEC_NUM = LOSS_AV_SEC.
469 RECODE LOSS_AV_SEC_NUM (SYSMIS=SYSMIS).
470 COMPUTE LOSS_AV_OPS_NUM = LOSS_AV_OPS.
471 RECODE LOSS_AV_OPS_NUM ( SYSMIS=SYSMIS).
472
473 **** New variables for checking H2: if Lottery comparisons of H2_1 to 5 are consistent with WTP for H2_6 to 8.
474 **** coding: 0 means consistency, 1 means contradiction.
475 ** Examine L9 and L10.
476 DO IF (H2_1 = 1 AND H2_6_1 > H2_7_1).
477     COMPUTE CONSISTENCY_L9 = 1.
478 ELSE IF (H2_1 = 1 AND H2_6_1 <= H2_7_1).
479     COMPUTE CONSISTENCY_L9 = 0.
480 ELSE IF (H2_1 = 2 AND H2_6_1 < H2_7_1).
481     COMPUTE CONSISTENCY_L10vsL9 = 1.
482 ELSE IF (H2_1 = 2 AND H2_6_1 >= H2_7_1).
483     COMPUTE CONSISTENCY_L10vsL9 = 0.
484 END IF.
485 ** Examine L10 and L11.
486 DO IF (H2_2 = 1 AND H2_7_1 > H2_8_1).
487     COMPUTE CONSISTENCY_L10vsL11 = 1.
488 ELSE IF (H2_2 = 1 AND H2_7_1 <= H2_8_1).
489     COMPUTE CONSISTENCY_L10vsL11 = 0.
490 ELSE IF (H2_2 = 2 AND H2_7_1 < H2_8_1).
491     COMPUTE CONSISTENCY_L11 = 1.
492 ELSE IF (H2_2 = 2 AND H2_7_1 >= H2_8_1).
493     COMPUTE CONSISTENCY_L11 = 0.
494 END IF.
495
496 **** also for cleaned data ****.
497 VARIABLE LEVEL S4 S12 S13 S14 S15 S16_1 S17_1 S19 S20_1 S21_1 (NOMINAL).
498
499 DO IF (S25_8_TEXT = 'english' OR S25_8_TEXT = 'English' OR S25_8_TEXT = 'ENGLISH').
500     COMPUTE S25 = 1.
501 ELSE.
502     COMPUTE S25 = 0.
503 END IF.
504
505 RECODE S17_1 (1=1) (2=1) (3=2) (4=2) (5=3) (6=3) (7=4) (8=4) (9=5) (10=5) (11=5) (12=SYSMIS)
506     (SYSMIS=SYSMIS) INTO S17.
```

A.1 Appendix: Experiment 1

```
507 VARIABLE LABELS S17 'Annual Salary'.
508 VARIABLE LABELS H2_6_1 'H2_6'.
509 VARIABLE LABELS H2_7_1 'H2_7'.
510 VARIABLE LABELS H2_8_1 'H2_8'.
511 EXECUTE.
512
513 RECODE S3_1 (1=0) (16=1) (2=2) (3=3) (4=4) (5=5) (6=6) (7=7) (8=8) (9=9) (10=10) (11=11)
      (12=12) (13=13) (14=14) (15=15).
514
515 ***** FILTER (If DUMMY=0, include case) *****
516 COMPUTE DUMMY=99.
517 DO IF H1_1>50 OR H1_2>50 OR H1_3>80 OR H1_4>80 OR H1_5>50 OR H1_6>50 OR H1_7>80 OR H1_8
      >80 OR H1_9>50 OR H1_10>50 OR H1_11>80 OR H1_12>80 OR H2Answer1 = '' OR MISSING(H1_1
      ).
518 COMPUTE DUMMY = 0.
519 ELSE.
520 COMPUTE DUMMY = 1.
521 END IF.
522 VARIABLE LEVEL DUMMY (NOMINAL).
523 FILTER BY DUMMY.
524
525 ***** Various Checks *****
526 ***** YourTotalDuration & S1 *****
527 FREQUENCIES S1
528 /ORDER=ANALYSIS.
529
530 ***** H1 and H2 WTP—lotteries *****
531 COMPUTE TimeH1A_3RND = RND(TimeH1A_3).
532 EXAMINE VARIABLES=H1_1_1 BY TimeH1A_3RND
533 /PLOT BOXPLOT STEMLEAF
534 /COMPARE GROUPS
535 /STATISTICS DESCRIPTIVES
536 /CINTERVAL 95
537 /MISSING LISTWISE
538 /NOTOTAL.
539 COMPUTE TimeH1A_3arRND = RND(TimeH1Aar_3).
540 EXAMINE VARIABLES=H1_1ar_1 BY TimeH1A_3arRND
541 /PLOT BOXPLOT STEMLEAF
542 /COMPARE GROUPS
543 /STATISTICS DESCRIPTIVES
544 /CINTERVAL 95
545 /MISSING LISTWISE
546 /NOTOTAL.
547
548 * Following Dr Mendosa, I do a Descriptive Statistics > Explore analysis with Steam&Leaf plot and Boxplots.
549 * There are initial conclusions on the Skewness and the Kurtosis (leptokurtosis or platukurtosis) of the
      distribution.
550 EXAMINE VARIABLES=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12
551 /PLOT BOXPLOT STEMLEAF
552 /COMPARE GROUPS
553 /STATISTICS DESCRIPTIVES
554 /CINTERVAL 95
555 /MISSING LISTWISE
556 /NOTOTAL.
557 *Boxplot of all Questions of H1 in the same Graphic (option: Data are Separate Variables).
558 EXAMINE VARIABLES=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12
559 /COMPARE VARIABLE
```

A.1 Appendix: Experiment 1

```
560 /PLOT=BOXPLOT
561 /STATISTICS=NONE
562 /NOTOTAL
563 /MISSING=PAIRWISE.
564 *Computes the z-values for the specified values AND SAVES them in new variables (starting with zVAR).
565 DESCRIPTIVES VARIABLES=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12
566 /SAVE
567 /STATISTICS=MEAN STDDEV MIN MAX.
568 *Descriptives for all variables of H1*.
569 EXAMINE VARIABLES=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12
570 /PLOT BOXPLOT STEMLEAF
571 /COMPARE GROUPS
572 /MESTIMATORS HUBER(1.339) ANDREW(1.34) HAMPEL(1.7,3.4,8.5) TUKEY(4.685)
573 /PERCENTILES(5,10,25,50,75,90,95) HAVERAGE
574 /STATISTICS DESCRIPTIVES EXTREME
575 /CINTERVAL 95
576 /MISSING LISTWISE
577 /NOTOTAL.
578
579 *Boxplot of all Questions of H1 in the same Graphic (option: Data are Separate Variables).
580 *Also used to define the limits for variable DUMMY.
581 EXAMINE VARIABLES=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
582 H2_7_1 H2_8_1
583 /COMPARE VARIABLE
584 /PLOT=BOXPLOT
585 /STATISTICS=NONE
586 /NOTOTAL
587 /MISSING=PAIRWISE.
588 ***** Order Effect ***** .
589 *Boxplot of all Questions of H1_i in the same Graphic by RISK_FIRST.
590 EXAMINE VARIABLES=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 BY
591 RISK_FIRST
592 /COMPARE VARIABLE
593 /PLOT=BOXPLOT
594 /STATISTICS=NONE
595 /NOTOTAL
596 /MISSING=PAIRWISE.
597 *This is to compare the first 6 variables of RtoA and AtoR for Risk & Ambiguity Aversion – as there is no
598 Order Effect.
599 EXAMINE VARIABLES=H1_1_1 H1_5_1 H1_9_1 H1_3_1 H1_7_1 H1_11_1
600 /COMPARE VARIABLE
601 /PLOT=BOXPLOT
602 /STATISTICS=NONE
603 /NOTOTAL
604 /MISSING=PAIRWISE.
605 EXAMINE VARIABLES=H1_4ar_1 H1_8ar_1 H1_12ar_1 H1_2ar_1 H1_6ar_1 H1_10ar_1
606 /COMPARE VARIABLE
607 /PLOT=BOXPLOT
608 /STATISTICS=NONE
609 /NOTOTAL
610 /MISSING=PAIRWISE.
611 *This is just additional information*.
612 *H1_10 and H1_12 from AtoR and RtoA look identical (there was no NP-test difference)*.
613 EXAMINE VARIABLES=H1_12ar_1 H1_10ar_1 H1_12_1 H1_10_1
614 /COMPARE VARIABLE
615 /PLOT=BOXPLOT
```

A.1 Appendix: Experiment 1

```
614 /STATISTICS=NONE
615 /NOTOTAL
616 /MISSING=PAIRWISE.
617 *H1_9 and H1_11 from AtoR and RtoA look identical (there was no NP—test difference)*.
618 EXAMINE VARIABLES=H1_9ar_1 H1_11ar_1 H1_9_1 H1_11_1
619 /COMPARE VARIABLE
620 /PLOT=BOXPLOT
621 /STATISTICS=NONE
622 /NOTOTAL
623 /MISSING=PAIRWISE.
624
625 *Nonparametric Tests: Independent Samples: H1 answers with Independent Variable = RISK_FIRST.
626 *Run the test with all cases.
627 NPTESTS
628 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12) GROUP (
        RISK_FIRST) MANN_WHITNEY
629 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
630 /CRITERIA ALPHA=0.05 CILEVEL=95.
631 *Additionally, I do an Outlier analysis to see if the outliers are the same subjects, and whether they should be
        excluded from the Mann—Whitney.
632 *The analysis is on the significant results of Mann—Whitney by RISK_FIRST.
633 *Result: subjects 6 and 21 are outliers in all 3 Variables. The Total Duration of the subjects is 24 and 30 mins,
        so does not imply fast completion.
634 EXAMINE VARIABLES=H1_1 H1_2 H1_4
635 /PLOT BOXPLOT STEMLEAF
636 /COMPARE GROUPS
637 /MESTIMATORS HUBER(1.339) ANDREW(1.34) HAMPEL(1.7,3.4,8.5) TUKEY(4.685)
638 /PERCENTILES(5,10,25,50,75,90,95) HAVERAGE
639 /STATISTICS DESCRIPTIVES EXTREME
640 /CINTERVAL 95
641 /MISSING LISTWISE
642 /NOTOTAL.
643
644 ***** HYPOTHESIS 1 – RISK and AMBIGUITY AVERSION *****.
645 ***** A) Between Subjects *****.
646 *****.
647 GRAPH
648 /LINE(SIMPLE)=VALUE(RiskAversionH1_1 RiskAversionH1_2 RiskAversionH1_3 RiskAversionH1_4).
649 GRAPH
650 /LINE(SIMPLE)=VALUE(RiskAversionH1_5 RiskAversionH1_6 RiskAversionH1_7 RiskAversionH1_8).
651 GRAPH
652 /LINE(SIMPLE)=VALUE(RiskAversionH1_9 RiskAversionH1_10 RiskAversionH1_11 RiskAversionH1_12).
653
654 *for all H1_i H2_j, deviations form mean, either 0 or lower by 25.
655 T—TEST
656 /TESTVAL=0
657 /MISSING=ANALYSIS
658 /VARIABLES=RiskAversionH1_1 RiskAversionH1_2 RiskAversionH1_3 RiskAversionH1_4
659 /CRITERIA=CI(.95).
660 T—TEST
661 /TESTVAL=0
662 /MISSING=ANALYSIS
663 /VARIABLES=RiskAversionH1_5 RiskAversionH1_6 RiskAversionH1_7 RiskAversionH1_8
664 /CRITERIA=CI(.95).
665 T—TEST
666 /TESTVAL=0
667 /MISSING=ANALYSIS
```

A.1 Appendix: Experiment 1

```
668 /VARIABLES=RiskAversionH1_9 RiskAversionH1_10 RiskAversionH1_11 RiskAversionH1_12
669 /CRITERIA=CI(.95).
670 T-TEST
671 /TESTVAL=0
672 /MISSING=ANALYSIS
673 /VARIABLES=RiskAversionH2_6 RiskAversionH2_7 RiskAversionH2_8
674 /CRITERIA=CI(.95).
675 * For checking outliers: .
676 EXAMINE VARIABLES=RiskAversionH1_1 RiskAversionH1_2 RiskAversionH1_3 RiskAversionH1_4
        RiskAversionH1_5 RiskAversionH1_6 RiskAversionH1_7 RiskAversionH1_8 RiskAversionH1_9
        RiskAversionH1_10 RiskAversionH1_11 RiskAversionH1_12
677 /COMPARE VARIABLE
678 /PLOT=BOXPLOT
679 /STATISTICS=NONE
680 /NOTOTAL
681 /MISSING=PAIRWISE.
682 * For deleting the outliers: .
683 EXAMINE VARIABLES=RiskAversionH1_9 RiskAversionH1_10 RiskAversionH1_11 RiskAversionH1_12
684 /COMPARE VARIABLE
685 /PLOT=BOXPLOT
686 /STATISTICS=NONE
687 /NOTOTAL
688 /MISSING=PAIRWISE.
689 EXAMINE VARIABLES= RiskAversionH2_6 RiskAversionH2_7 RiskAversionH2_8
690 /PLOT=BOXPLOT
691 /STATISTICS=NONE
692 /NOTOTAL
693 /MISSING=PAIRWISE.
694 * another way: Detecting OUTLIERS from z-scores: if cum. % of Std. Deviation > 1.96 is about 5%, then we
        are fine! *.
695 * H1_1 *.
696 DESCRIPTIVES
697 VARIABLES=H1_1/SAVE.
698 COMPUTE zH1_1=abs(zH1_1).
699 RECODE zH1_1 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
700 VALUE LABELS zH1_1
701 4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
        Outliers (z>3.29)'.
702 FREQUENCIES
703 VARIABLES=zH1_1
704 /ORDER=ANALYSIS.
705 * H1_2 *.
706 DESCRIPTIVES
707 VARIABLES=H1_2/SAVE.
708 COMPUTE zH1_2=abs(zH1_2).
709 RECODE zH1_2 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
710 VALUE LABELS zH1_2
711 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
        '.
712 FREQUENCIES
713 VARIABLES=zH1_2
714 /ORDER=ANALYSIS.
715 * H1_3 *.
716 DESCRIPTIVES
717 VARIABLES=H1_3/SAVE.
```

A.1 Appendix: Experiment 1

```
718 COMPUTE zH1_3=abs(zH1_3).
719 RECODE zH1_3 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
720 VALUE LABELS zH1_3
721 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
722 FREQUENCIES
723 VARIABLES=zH1_3
724 /ORDER=ANALYSIS.
725 * H1.4 *.
726 DESCRIPTIVES
727 VARIABLES=H1_4/SAVE.
728 COMPUTE zH1_4=abs(zH1_4).
729 RECODE zH1_4 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
730 VALUE LABELS zH1_4
731 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
732 FREQUENCIES
733 VARIABLES=zH1_4
734 /ORDER=ANALYSIS.
735 * H1.5 *.
736 DESCRIPTIVES
737 VARIABLES=H1_5/SAVE.
738 COMPUTE zH1_5=abs(zH1_5).
739 RECODE zH1_5 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
740 VALUE LABELS zH1_5
741 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
742 FREQUENCIES
743 VARIABLES=zH1_5
744 /ORDER=ANALYSIS.
745 * H1.6 *.
746 DESCRIPTIVES
747 VARIABLES=H1_6/SAVE.
748 COMPUTE zH1_6=abs(zH1_6).
749 RECODE zH1_6 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
750 VALUE LABELS zH1_6
751 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
752 FREQUENCIES
753 VARIABLES=zH1_6
754 /ORDER=ANALYSIS.
755 * H1.7 *.
756 DESCRIPTIVES
757 VARIABLES=H1_7/SAVE.
758 COMPUTE zH1_7=abs(zH1_7).
759 RECODE zH1_7 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
760 VALUE LABELS zH1_7
761 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
762 FREQUENCIES
763 VARIABLES=zH1_7
764 /ORDER=ANALYSIS.
```

A.1 Appendix: Experiment 1

```
765 * H1_8 *.
766 DESCRIPTIVES
767 VARIABLES=H1_8/SAVE.
768 COMPUTE zH1_8=abs(zH1_8).
769 RECODE zH1_8 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
770 VALUE LABELS zH1_8
771 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
772 FREQUENCIES
773 VARIABLES=zH1_8
774 /ORDER=ANALYSIS.
775 * H1_9 *.
776 DESCRIPTIVES
777 VARIABLES=H1_9/SAVE.
778 COMPUTE zH1_8=abs(zH1_9).
779 RECODE zH1_9 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
780 VALUE LABELS zH1_9
781 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
782 FREQUENCIES
783 VARIABLES=zH1_9
784 /ORDER=ANALYSIS.
785 * H1_10 *.
786 DESCRIPTIVES
787 VARIABLES=H1_10/SAVE.
788 COMPUTE zH1_10=abs(zH1_10).
789 RECODE zH1_10 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 =
4).
790 VALUE LABELS zH1_10
791 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
792 FREQUENCIES
793 VARIABLES=zH1_10
794 /ORDER=ANALYSIS.
795 * H1_11 *.
796 DESCRIPTIVES
797 VARIABLES=H1_11/SAVE.
798 COMPUTE zH1_11=abs(zH1_11).
799 RECODE zH1_11 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 =
4).
800 VALUE LABELS zH1_11
801 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
802 FREQUENCIES
803 VARIABLES=zH1_11
804 /ORDER=ANALYSIS.
805 * H1_12 *.
806 DESCRIPTIVES
807 VARIABLES=H1_12/SAVE.
808 COMPUTE zH1_12=abs(zH1_12).
809 RECODE zH1_12 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 =
4).
810 VALUE LABELS zH1_12
811 4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
.
```

A.1 Appendix: Experiment 1

```
812 FREQUENCIES
813   VARIABLES=zH1_12
814 /ORDER=ANALYSIS.
815 * H2.6.1 *.
816 DESCRIPTIVES
817 VARIABLES=H2_6.1/SAVE.
818 COMPUTE zH2_6.1=abs(zH2_6.1).
819 RECODE zH2_6.1 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 =
820 4).
821 VALUE LABELS zH2_6.1
822   4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
823   !.
824 FREQUENCIES
825   VARIABLES=zH2_6.1
826 /ORDER=ANALYSIS.
827 * H2.7.1 *.
828 DESCRIPTIVES
829 VARIABLES=H2_7.1/SAVE.
830 COMPUTE zH2_7.1=abs(zH2_7.1).
831 RECODE zH2_7.1 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 =
832 4).
833 VALUE LABELS zH2_7.1
834   4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
835   !.
836 FREQUENCIES
837   VARIABLES=zH2_7.1
838 /ORDER=ANALYSIS.
839 * H2.8.1 *.
840 DESCRIPTIVES
841 VARIABLES=H2_8.1/SAVE.
842 COMPUTE zH2_8.1=abs(zH2_8.1).
843 RECODE zH2_8.1 (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 =
844 4).
845 VALUE LABELS zH2_8.1
846   4 'Normal range' 3 'Potential Outliers (z>1.96)' 2 'Probabe Outliers (z>2.58)' 1 'Extreme Outliers (z>3.29)
847   !.
848 FREQUENCIES
849   VARIABLES=zH2_8.1
850 /ORDER=ANALYSIS.
851 ***** B) Within Subjects *****
852 *****
853 ***1st Categorisation by the same Expected Value.***
854 **Nonparametric Tests: Related Samples, many conditions.
855 **Group A.
856 NPTESTS
857 /RELATED TEST(RiskAversionH1_1 RiskAversionH1_2 RiskAversionH1_3 RiskAversionH1_4)
858 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
859 /CRITERIA ALPHA=0.05 CILEVEL=95.
860 *FRIEDMAN.
861 NPAR TESTS
862 /FRIEDMAN=RiskAversionH1_1 RiskAversionH1_2 RiskAversionH1_3 RiskAversionH1_4
863 /STATISTICS QUANTILES
864 /MISSING LISTWISE.
865 NPAR TESTS
866 /WILCOXON=RiskAversionH1_1 RiskAversionH1_1 RiskAversionH1_1 RiskAversionH1_2 RiskAversionH1_2
867 RiskAversionH1_3 WITH RiskAversionH1_2 RiskAversionH1_3 RiskAversionH1_4 RiskAversionH1_3
```


A.1 Appendix: Experiment 1

```
863 RiskAversionH1_4 RiskAversionH1_4 (PAIRED)
864 /MISSING ANALYSIS.
865 **Group B.
866 NPTESTS
867 /RELATED TEST(RiskAversionH1_5 RiskAversionH1_6 RiskAversionH1_7 RiskAversionH1_8)
868 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
869 /CRITERIA ALPHA=0.05 CILEVEL=95.
870 NPAR TESTS
871 /FRIEDMAN=RiskAversionH1_5 RiskAversionH1_6 RiskAversionH1_7 RiskAversionH1_8
872 /MISSING LISTWISE.
873 NPAR TESTS
874 /WILCOXON=RiskAversionH1_5 RiskAversionH1_5 RiskAversionH1_5 RiskAversionH1_6 RiskAversionH1_6
875 RiskAversionH1_7 WITH RiskAversionH1_6 RiskAversionH1_7 RiskAversionH1_8 RiskAversionH1_7
876 RiskAversionH1_8 RiskAversionH1_8 (PAIRED)
877 /MISSING ANALYSIS.
878 **Group C.
879 NPTESTS
880 /RELATED TEST(RiskAversionH1_9 RiskAversionH1_10 RiskAversionH1_11 RiskAversionH1_12)
881 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
882 /CRITERIA ALPHA=0.05 CILEVEL=95.
883 NPAR TESTS
884 /FRIEDMAN=RiskAversionH1_9 RiskAversionH1_10 RiskAversionH1_11 RiskAversionH1_12
885 /MISSING LISTWISE.
886 NPAR TESTS
887 /WILCOXON=RiskAversionH1_9 RiskAversionH1_9 RiskAversionH1_9 RiskAversionH1_10 RiskAversionH1_10
888 RiskAversionH1_11 WITH RiskAversionH1_10 RiskAversionH1_11 RiskAversionH1_12 RiskAversionH1_11
889 RiskAversionH1_12 RiskAversionH1_12 (PAIRED)
890 /MISSING ANALYSIS.
891 **Group D.
892 NPTESTS
893 /RELATED TEST(RiskAversionH2_6 RiskAversionH2_7 RiskAversionH2_8)
894 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
895 /CRITERIA ALPHA=0.05 CILEVEL=95.
896 NPAR TESTS
897 /FRIEDMAN=RiskAversionH2_6 RiskAversionH2_7 RiskAversionH2_8
898 /MISSING LISTWISE.
899 NPAR TESTS
900 /WILCOXON=RiskAversionH2_6 RiskAversionH2_6 RiskAversionH2_7 WITH RiskAversionH2_7
901 RiskAversionH2_8 RiskAversionH2_8 (PAIRED)
902 /MISSING ANALYSIS.
903
904 ***2nd Categorisation by the lottery nature: risky, ambig in probs, ambig in outcomes, ambig in probs and
905 outcomes***.
906 **Nonparametric Tests: Related Samples, many conditions.
907 **Group E.
908 *actual risk aversion values (only Group E).
909 NPTESTS
910 /RELATED TEST(RiskAversionH1_1 RiskAversionH1_5 RiskAversionH1_9)
911 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
912 /CRITERIA ALPHA=0.05 CILEVEL=95.
913 NPAR TESTS
914 /WILCOXON=RiskAversionH1_1 RiskAversionH1_1 RiskAversionH1_5 WITH
915 RiskAversionH1_5 RiskAversionH1_9 RiskAversionH1_9 (PAIRED)
916 /MISSING ANALYSIS.
917 EXAMINE VARIABLES=RiskAversionH1_1 RiskAversionH1_5 RiskAversionH1_9
918 /COMPARE VARIABLE
919 /PLOT=BOXPLOT
```

A.1 Appendix: Experiment 1

```
919 /STATISTICS=NONE
920 /NOTOTAL
921 /MISSING=PAIRWISE.
922 *ratios (only Group E).
923 NPTESTS
924 /RELATED TEST(RiskAversionH1_1ratio RiskAversionH1_5ratio RiskAversionH1_9ratio)
925 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
926 /CRITERIA ALPHA=0.05 CILEVEL=95.
927 NPAR TESTS
928 /WILCOXON=RiskAversionH1_1ratio RiskAversionH1_1ratio RiskAversionH1_5ratio WITH
929 RiskAversionH1_5ratio RiskAversionH1_9ratio RiskAversionH1_9ratio (PAIRED)
930 /MISSING ANALYSIS.
931 EXAMINE VARIABLES=RiskAversionH1_1ratio RiskAversionH1_5ratio RiskAversionH1_9ratio
932 /COMPARE VARIABLE
933 /PLOT=BOXPLOT
934 /STATISTICS=NONE
935 /NOTOTAL
936 /MISSING=PAIRWISE.
937 **Group F.
938 NPTESTS
939 /RELATED TEST(RiskAversionH1_2ratio RiskAversionH1_6ratio RiskAversionH1_10ratio)
940 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
941 /CRITERIA ALPHA=0.05 CILEVEL=95.
942 NPAR TESTS
943 /WILCOXON=RiskAversionH1_2ratio RiskAversionH1_2ratio RiskAversionH1_6ratio WITH
944 RiskAversionH1_6ratio RiskAversionH1_10ratio RiskAversionH1_10ratio (PAIRED)
945 /MISSING ANALYSIS.
946 EXAMINE VARIABLES=RiskAversionH1_2ratio RiskAversionH1_6ratio RiskAversionH1_10ratio
947 /COMPARE VARIABLE
948 /PLOT=BOXPLOT
949 /STATISTICS=NONE
950 /NOTOTAL
951 /MISSING=PAIRWISE.
952 **Group G.
953 NPTESTS
954 /RELATED TEST(RiskAversionH1_3ratio RiskAversionH1_7ratio RiskAversionH1_11ratio)
955 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
956 /CRITERIA ALPHA=0.05 CILEVEL=95.
957 NPAR TESTS
958 /WILCOXON=RiskAversionH1_3ratio RiskAversionH1_3ratio RiskAversionH1_7ratio WITH
959 RiskAversionH1_7ratio RiskAversionH1_11ratio RiskAversionH1_11ratio (PAIRED)
960 /MISSING ANALYSIS.
961 EXAMINE VARIABLES=RiskAversionH1_3ratio RiskAversionH1_7ratio RiskAversionH1_11ratio
962 /COMPARE VARIABLE
963 /PLOT=BOXPLOT
964 /STATISTICS=NONE
965 /NOTOTAL
966 /MISSING=PAIRWISE.
967 **Group H.
968 NPTESTS
969 /RELATED TEST(RiskAversionH1_4ratio RiskAversionH1_8ratio RiskAversionH1_12ratio)
970 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
971 /CRITERIA ALPHA=0.05 CILEVEL=95.8.
972 NPAR TESTS
973 /WILCOXON=RiskAversionH1_4ratio RiskAversionH1_4ratio RiskAversionH1_8ratio WITH
974 RiskAversionH1_8ratio RiskAversionH1_12ratio RiskAversionH1_12ratio (PAIRED)
975 /MISSING ANALYSIS.
```

A.1 Appendix: Experiment 1

```
976 EXAMINE VARIABLES=RiskAversionH1_4ratio RiskAversionH1_8ratio RiskAversionH1_12ratio
977 /COMPARE VARIABLE
978 /PLOT=BOXPLOT
979 /STATISTICS=NONE
980 /NOTOTAL
981 /MISSING=PAIRWISE.
982
983 GRAPH
984 /BAR(SIMPLE)=MEAN(RiskAversionH1_1) MEAN(RiskAversionH1_2) MEAN(RiskAversionH1_3) MEAN(
RiskAversionH1_4) MEAN(RiskAversionH1_5) MEAN(RiskAversionH1_6) MEAN(RiskAversionH1_7)
MEAN(RiskAversionH1_8)
985 MEAN(RiskAversionH1_9) MEAN(RiskAversionH1_10) MEAN(RiskAversionH1_11) MEAN(
RiskAversionH1_12) MEAN(RiskAversionH2_6) MEAN(RiskAversionH2_7) MEAN(RiskAversionH2_8)
986 /MISSING=LISTWISE
987 /INTERVAL CI(95.0).
988 GRAPH
989 /BAR(SIMPLE)=MEAN(RiskAversionH2_6) MEAN(RiskAversionH2_7) MEAN(RiskAversionH2_8)
990 /MISSING=LISTWISE
991 /INTERVAL CI(95.0).
992 *bonferoni correction.
993
994 ***** H2 *****
995 *****
996 *** 1) Lottery comparisons ***.
997 EXAMINE VARIABLES=H2_6_1 H2_7_1 H2_8_1
998 /COMPARE VARIABLE
999 /PLOT=BOXPLOT
1000 /STATISTICS=NONE
1001 /NOTOTAL
1002 /MISSING=PAIRWISE.
1003 EXAMINE VARIABLES=RiskAversionH2_6 RiskAversionH2_7 RiskAversionH2_8
1004 /COMPARE VARIABLE
1005 /PLOT=BOXPLOT
1006 /STATISTICS=NONE
1007 /NOTOTAL
1008 /MISSING=PAIRWISE.
1009 EXAMINE VARIABLES=RiskAversionH2_6ratio RiskAversionH2_7ratio RiskAversionH2_8ratio
1010 /COMPARE VARIABLE
1011 /PLOT=BOXPLOT
1012 /STATISTICS=NONE
1013 /NOTOTAL
1014 /MISSING=PAIRWISE.
1015
1016 MEANS TABLES=RiskAversionH2_6 RiskAversionH2_7 RiskAversionH2_8
1017 /CELLS MEAN COUNT STDDEV.
1018
1019 FREQUENCIES VARIABLES=H2_1 H2_2 H2_3 H2_4 H2_5
1020 /ORDER=ANALYSIS.
1021 FREQUENCIES VARIABLES=H2_6_1 H2_7_1 H2_8_1
1022 /HISTOGRAM
1023 /ORDER=ANALYSIS.
1024 ** WTP for Lottery 9 and 10 BY Comparison Lottery9 OR 10 **.
1025 EXAMINE VARIABLES=H2_6_1 H2_7_1 BY H2_1
1026 /COMPARE VARIABLE
1027 /PLOT=BOXPLOT
1028 /STATISTICS=NONE
1029 /NOTOTAL
```

A.1 Appendix: Experiment 1

```

1030 /MISSING=PAIRWISE.
1031 ** WTP for Lottery 10 and 11 BY Comparison Lottery10 OR 11 **.
1032 EXAMINE VARIABLES=H2_7_1 H2_8_1 BY H2_2
1033 /COMPARE VARIABLE
1034 /PLOT=BOXPLOT
1035 /STATISTICS=NONE
1036 /NOTOTAL
1037 /MISSING=PAIRWISE.
1038 *Risk Aversion for each of the 3 WTP questions: .
1039 GRAPH
1040 /LINE(SIMPLE)=VALUE(RiskAversionH2_6_1 RiskAversionH2_7_1 RiskAversionH2_8_1).
1041 EXAMINE VARIABLES=RiskAversionH2_6_1 RiskAversionH2_7_1 RiskAversionH2_8_1
1042 /COMPARE VARIABLE
1043 /PLOT=BOXPLOT
1044 /STATISTICS=NONE
1045 /NOTOTAL
1046 /MISSING=PAIRWISE.
1047 *chi-2 for Lottery comparisons, amongst PROS and STUDENTS.
1048 CROSSTABS
1049 /TABLES=H2_1 H2_2 H2_3 H2_4 H2_5 BY S1
1050 /FORMAT=AVALUE TABLES
1051 /STATISTICS=CHISQ PHI
1052 /CELLS=COUNT EXPECTED
1053 /COUNT ROUND CELL.
1054
1055 **** 2) Preferred lotteries and stated WTP ****.
1056 FREQUENCIES CONSISTENCY_L9 CONSISTENCY_L10vsL9 CONSISTENCY_L10vsL11
1057 CONSISTENCY_L11
1058 /ORDER=ANALYSIS.
1059 *chi-2 for INCONSISTENCY in Lottery Comparisons and WTP, amongst PROS and STUDENTS.
1060 CROSSTABS
1061 /TABLES=CONSISTENCY_L9 CONSISTENCY_L10vsL9 CONSISTENCY_L10vsL11 CONSISTENCY_L11 BY S1
1062 /FORMAT=AVALUE TABLES
1063 /STATISTICS=CHISQ PHI
1064 /CELLS=COUNT EXPECTED
1065 /COUNT ROUND CELL.
1066 * within-subjects for Lottery Comparison H2_1 to 5 by some ordinal (continuous) characteristic)*.
1067 NPTESTS
1068 /RELATED TEST(EV_H2_6 EV_H2_7 EV_H2_8)
1069 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1070 /CRITERIA ALPHA=0.05 CILEVEL=95.
1071 NPAR TESTS
1072 /WILCOXON=EV_H2_6 EV_H2_6 EV_H2_7 WITH
1073 EV_H2_7 EV_H2_8 EV_H2_8 (PAIRED)
1074 /MISSING ANALYSIS.
1075 EXAMINE VARIABLES=EV_H2_6 EV_H2_7 EV_H2_8
1076 /COMPARE VARIABLE
1077 /PLOT=BOXPLOT
1078 /STATISTICS=NONE
1079 /NOTOTAL
1080 /MISSING=PAIRWISE.
1081 ***** H3 *****.
1082 **** (1) Hypothesis 3 and Willingness-To-Pay *****.
1083 *Boxplot of all H1.i and the three WTP Questions of H2, by H3Group – allows to compare the 2 Groups (H3
1084 and no H3).
1085 EXAMINE VARIABLES=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 BY H3Group

```

A.1 Appendix: Experiment 1

```
1085 /COMPARE VARIABLE
1086 /PLOT=BOXPLOT
1087 /STATISTICS=NONE
1088 /NOTOTAL
1089 /MISSING=PAIRWISE.
1090 EXAMINE VARIABLES=H2_6.1 H2.7.1 H2.8.1 BY H3Group
1091 /COMPARE VARIABLE
1092 /PLOT=BOXPLOT
1093 /STATISTICS=NONE
1094 /NOTOTAL
1095 /MISSING=PAIRWISE.
1096 *Boxplot of all H1i, by two axes: H3Group and RISK_FIRST – allows to (visually) compare the 4 Groups.
1097 *Q: how to find significance? i.e. how to do Mann–whitney for 2 Ind Vars: H3Group AND RISK_FIRST?.
1098 EXAMINE VARIABLES=H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 BY H3Group
1099 /COMPARE VARIABLE
1100 /PLOT=BOXPLOT
1101 /STATISTICS=NONE
1102 /NOTOTAL
1103 /PANEL ROWVAR=RISK_FIRST ROWOP=CROSS
1104 /MISSING=PAIRWISE.
1105 *An additional Boxplot –only for case H1.1– (Descriptives>Explore) to see how H1.1 Outliers are FACTORed
    by H3Group.
1106 *Comment: this is an initial Visual aid, before the Mann–Whitney is run, but it can be used for other vars.
1107 EXAMINE VARIABLES=H1.1 BY H3Group
1108 /PLOT BOXPLOT STEMLEAF
1109 /COMPARE GROUPS
1110 /STATISTICS DESCRIPTIVES
1111 /CINTERVAL 95
1112 /MISSING LISTWISE
1113 /NOTOTAL.
1114 *Nonparametric Tests: Independent Samples: H1 answers need to be consolidated first – ok! Now, they shold
    not be Categorical.
1115 NPTESTS
1116 /INDEPENDENT TEST (H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1
    H2.7.1 H2.8.1) GROUP (H3Group) MANN_WHITNEY
1117 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1118 /CRITERIA ALPHA=0.05 CILEVEL=95.
1119
1120 ***** (2) Hypothesis 3 and Lottery Comparison *****.
1121 *Stem and Leaf & Bars for Lottery Comparisons: H2.1 to H2.5 by factor H3.
1122 EXAMINE VARIABLES=H2.1 H2.2 H2.3 H2.4 H2.5 BY H3Group
1123 /PLOT BOXPLOT STEMLEAF
1124 /COMPARE GROUPS
1125 /STATISTICS DESCRIPTIVES
1126 /CINTERVAL 95
1127 /MISSING LISTWISE
1128 /NOTOTAL.
1129 *Nonparametric Tests: H2.1 to H2.5, by H3Group.
1130 NPTESTS
1131 /INDEPENDENT TEST (H2.1 H2.2 H2.3 H2.4 H2.5) GROUP (H3Group) MANN_WHITNEY
1132 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1133 /CRITERIA ALPHA=0.05 CILEVEL=95.
1134
1135 ***** (3) Hypothesis 3 and Security VS Operability preferences *****.
1136 *** (a) Simple preference between Security and Operability.
1137 NPTESTS
1138 /INDEPENDENT TEST (H5.1.1.1) GROUP (H3Group) MANN_WHITNEY
```

A.1 Appendix: Experiment 1

```
1139 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1140 /CRITERIA ALPHA=0.05 CILEVEL=95.
1141 *** (b) Switching point of utility.
1142 *GRAPH
1143 */HISTOGRAM=SWITCHPOINT_SEC.
1144 *GRAPH
1145 */HISTOGRAM= SWITCHPOINT_OPS.
1146 NPTESTS
1147 /INDEPENDENT TEST (SWITCHPOINT_SEC_NUM SWITCHPOINT_OPS_NUM) GROUP (H3Group)
      MANN_WHITNEY
1148 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1149 /CRITERIA ALPHA=0.05 CILEVEL=95.
1150 *** (c) Relative Loss Aversion between Security and Operability.
1151 NPTESTS
1152 /INDEPENDENT TEST (LOSS_AV_SEC_NUM LOSS_AV_OPS_NUM) GROUP (H3Group)
      MANN_WHITNEY
1153 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1154 /CRITERIA ALPHA=0.05 CILEVEL=95.
1155
1156 ***** (4) Hypothesis 3 and Survey Responses *****
1157 * H3 and Personal Risk Taking *.
1158 NPTESTS
1159 /INDEPENDENT TEST (S5_1) GROUP (H3Group) MANN_WHITNEY
1160 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1161 /CRITERIA ALPHA=0.05 CILEVEL=95.
1162 * H3 and Worry about security incident in working environment *.
1163 NPTESTS
1164 /INDEPENDENT TEST (S6_1) GROUP (H3Group) MANN_WHITNEY
1165 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1166 /CRITERIA ALPHA=0.05 CILEVEL=95.
1167 * H3 and Worry about unknown threats *.
1168 NPTESTS
1169 /INDEPENDENT TEST (S7_1) GROUP (H3Group) MANN_WHITNEY
1170 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1171 /CRITERIA ALPHA=0.05 CILEVEL=95.
1172 * H3 and Trade-off between Security and Operations today *.
1173 NPTESTS
1174 /INDEPENDENT TEST (S8_1) GROUP (H3Group) MANN_WHITNEY
1175 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1176 /CRITERIA ALPHA=0.05 CILEVEL=95.
1177 * H3 and Trade-off between Security and Operations in working envoronment *.
1178 NPTESTS
1179 /INDEPENDENT TEST (S9_1) GROUP (H3Group) MANN_WHITNEY
1180 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1181 /CRITERIA ALPHA=0.05 CILEVEL=95.
1182 * H3 and Worry Information Security closness to business objectives *.
1183 NPTESTS
1184 /INDEPENDENT TEST (S10_1) GROUP (H3Group) MANN_WHITNEY
1185 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1186 /CRITERIA ALPHA=0.05 CILEVEL=95.
1187 * H3 and How willing they are to sacrifice Operations for Security *.
1188 NPTESTS
1189 /INDEPENDENT TEST (S11_1) GROUP (H3Group) MANN_WHITNEY
1190 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1191 /CRITERIA ALPHA=0.05 CILEVEL=95.
1192 *initial Mann-Whitney test with all valid values of ÎŰ1.1.
1193 NPTESTS
```

A.1 Appendix: Experiment 1

```
1194 /INDEPENDENT TEST (H1_1) GROUP (H3Group) MANN_WHITNEY
1195 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1196 /CRITERIA ALPHA=0.05 CILEVEL=95..
1197 *  $\hat{U}$ 1_1 Skewness and Kurtosis Boxplot.
1198 EXAMINE VARIABLES=H1_1
1199 /PLOT BOXPLOT STEMLEAF
1200 /COMPARE GROUPS
1201 /STATISTICS DESCRIPTIVES
1202 /CINTERVAL 95
1203 /MISSING LISTWISE
1204 /NOTOTAL.
1205 *Mann-Whitney test  $\hat{U}$ 1_1 EXCLUDING the OUTLIERS.
1206 NPTESTS
1207 /INDEPENDENT TEST (H1_1) GROUP (H3Group) MANN_WHITNEY
1208 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1209 /CRITERIA ALPHA=0.05 CILEVEL=95.
1210 **** *****.
1211 DATASET DISPLAY.
1212
1213 ***** H4 *****.
1214 FREQUENCIES VARIABLES=H5_1_1_1 SWITCHPOINT_SEC SWITCHPOINT_OPS LOSS_AV_SEC
1215     LOSS_AV_OPS
1216     /HISTOGRAM
1217     /ORDER=ANALYSIS.
1218 FREQUENCIES VARIABLES=SWITCHPOINT_SEC SWITCHPOINT_OPS
1219     /FORMAT=DVALUE
1220     /ORDER=ANALYSIS.
1221 ***** SURVEY *****.
1222 **** A) Descriptive Statistics *****.
1223 FREQUENCIES VARIABLES=S1 S2_1 S3_1 S4 S5_1 S6_1 S7_1 S8_1 S9_1 S10_1 S11_1 S12 S13 S14 S15 S16_1
1224     S17_1 S18_1 S19 S20_1 S21_1 S22_1 S23_8.TEXT S24_8.TEXT S25_8.TEXT
1225     /HISTOGRAM
1226     /ORDER=ANALYSIS.
1227 FREQUENCIES VARIABLES=S5_1
1228     /HISTOGRAM
1229     /ORDER=ANALYSIS.
1230 FREQUENCIES VARIABLES=S18
1231     /HISTOGRAM
1232     /ORDER=ANALYSIS.
1233 GRAPH
1234     /PIE=COUNT BY S22_1.
1235 GRAPH
1236     /PIE=COUNT BY S25_8.TEXT.
1237 GRAPH
1238     /PIE=COUNT BY S4.
1239 **** B) Spearman correlations *****.
1240 ** Spearman: Quant with Quant variables **.
1241 NONPAR CORR
1242     /VARIABLES=S2_1 S3_1 S5_1 S6_1 S7_1 S8_1 S9_1 S10_1 S11_1 S18_1 S22_1 H1_1 H1_2 H1_3 H1_4 H1_5
1243         H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1244     /PRINT=SPEARMAN TWOTAIL NOSIG
1245     /MISSING=PAIRWISE.
1246 * Risk taking correlations with WTP *.
1247 NONPAR CORR
1248     /VARIABLES=S5_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1
```

A.1 Appendix: Experiment 1

```

      H2.8.1
1248 /PRINT=SPEARMAN TWOTAIL NOSIG
1249 /MISSING=PAIRWISE.
1250 GRAPH
1251 /SCATTERPLOT(BIVAR)=H1.9 WITH S5.1
1252 /MISSING=LISTWISE.
1253
1254 * Unidentified Threats correlations with WTP *.
1255 NONPAR CORR
1256 /VARIABLES=S7.1 H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1 H2.7.1
      H2.8.1
1257 /PRINT=SPEARMAN TWOTAIL NOSIG
1258 /MISSING=PAIRWISE.
1259 GRAPH
1260 /SCATTERPLOT(BIVAR)=H1.9 WITH S7.1
1261 /MISSING=LISTWISE.
1262
1263 * Years of Sec Experience correlations with WTP *.
1264 NONPAR CORR
1265 /VARIABLES=S2.1 H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1 H2.7.1
      H2.8.1
1266 /PRINT=SPEARMAN TWOTAIL NOSIG
1267 /MISSING=PAIRWISE.
1268 GRAPH
1269 /SCATTERPLOT(BIVAR)=H1.9 WITH S7.1
1270 /MISSING=LISTWISE.
1271
1272 *** C) Mann-Whitney: Quant with binary Qual variables **.
1273 * Have experienced an incident? S4 * *I have included: Yes=1, No=2, n/a=3, so this test has to move to K-W*.
1274 *NPTESTS
1275 /INDEPENDENT TEST (H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1
      H2.7.1 H2.8.1) GROUP (S4) MANN_WHITNEY
1276 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1277 /CRITERIA ALPHA=0.05 CILEVEL=95.
1278 * Independent decision-making S13 *.
1279 NPTESTS
1280 /INDEPENDENT TEST (H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1
      H2.7.1 H2.8.1) GROUP (S13) MANN_WHITNEY
1281 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1282 /CRITERIA ALPHA=0.05 CILEVEL=95.
1283 * More CIA at work needed S14 *.
1284 NPTESTS
1285 /INDEPENDENT TEST (H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1
      H2.7.1 H2.8.1) GROUP (S14) MANN_WHITNEY
1286 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1287 /CRITERIA ALPHA=0.05 CILEVEL=95.
1288 * Gender S19*.
1289 NPTESTS
1290 /INDEPENDENT TEST (H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1
      H2.7.1 H2.8.1) GROUP (S19) MANN_WHITNEY
1291 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1292 /CRITERIA ALPHA=0.05 CILEVEL=95.
1293 * Mother tongue S25 *.
1294 NPTESTS
1295 /INDEPENDENT TEST (H1.1 H1.2 H1.3 H1.4 H1.5 H1.6 H1.7 H1.8 H1.9 H1.10 H1.11 H1.12 H2.6.1
      H2.7.1 H2.8.1) GROUP (S25) MANN_WHITNEY
1296 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
```


A.1 Appendix: Experiment 1

```
1297 /CRITERIA ALPHA=0.05 CILEVEL=95.
1298 * Student or Professional S1 *.
1299 NPTESTS
1300 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
      H2_7_1 H2_8_1) GROUP (S1) MANN_WHITNEY
1301 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1302 /CRITERIA ALPHA=0.05 CILEVEL=95.
1303
1304 ** D) Kruskal–Wallis: Quant with many–categories Qual variables **.
1305 * Have experienced an incident? S4 *.
1306 NPTESTS
1307 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
      H2_7_1 H2_8_1) GROUP (S4) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1308 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1309 /CRITERIA ALPHA=0.05 CILEVEL=95.
1310 * Job title (categories=5) S12 *.
1311 NPTESTS
1312 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
      H2_7_1 H2_8_1) GROUP (S12) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1313 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1314 /CRITERIA ALPHA=0.05 CILEVEL=95.
1315 * Who makes decision in the company? (categories=5) S15_1 *.
1316 NPTESTS
1317 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
      H2_7_1 H2_8_1) GROUP (S15) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1318 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1319 /CRITERIA ALPHA=0.05 CILEVEL=95.
1320 * Number of employees (categories=6) S16_1 *.
1321 NPTESTS
1322 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
      H2_7_1 H2_8_1) GROUP (S16) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1323 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1324 /CRITERIA ALPHA=0.05 CILEVEL=95.
1325 * Annual salary (categories=5) S17_1 *.
1326 NPTESTS
1327 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
      H2_7_1 H2_8_1) GROUP (S17) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1328 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1329 /CRITERIA ALPHA=0.05 CILEVEL=95.
1330 * Educational level (categories=4) S20_1*.
1331 NPTESTS
1332 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6_1
      H2_7_1 H2_8_1) GROUP (S20_1)
1333 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1334 /CRITERIA ALPHA=0.05 CILEVEL=95.
1335 *new (Legacy).
1336 NPAR TESTS
1337 /K–W=H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6 H2_7 H2_8 BY S20(1
      4)
1338 /STATISTICS DESCRIPTIVES QUARTILES
1339 /MISSING ANALYSIS.
1340 *new (Nonparametric Tests: Independent Samples). – Significant [no split data].
1341 NPTESTS
1342 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2_6
      H2_7 H2_8)
1343 GROUP (S20) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1344 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
```

A.1 Appendix: Experiment 1

```
1345 /CRITERIA ALPHA=0.05 CILEVEL=95.
1346 * Marital status (categories=7).
1347 NPTESTS
1348 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2.6
      H2_7 H2.8) GROUP (S21) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1349 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1350 /CRITERIA ALPHA=0.05 CILEVEL=95.
1351 * SwitchingPoints & Loss Aversion BY Job Title status (categories=5) [None is Sig. if I do not use the missing
      =99 coding and system missing=system missing].
1352 NPTESTS
1353 /INDEPENDENT TEST (SWITCHPOINT_SEC_NUM SWITCHPOINT_OPS_NUM LOSS_AV_SEC_NUM
      LOSS_AV_OPS_NUM) GROUP (S12) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1354 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1355 /CRITERIA ALPHA=0.05 CILEVEL=95.
1356 * More CIA (1=Yes, 2=No, 3=n\2).
1357 NPTESTS
1358 /INDEPENDENT TEST (H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8 H1_9 H1_10 H1_11 H1_12 H2.6
      H2_7 H2.8) GROUP (S14) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
1359 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
1360 /CRITERIA ALPHA=0.05 CILEVEL=95.
1361
1362 **** E) Chi-square (Pearson): Qual with Qual [the first Sig. is the one] ****.
1363 * Sec VS OPS BY Past Incident*.
1364 CROSSTABS
1365 /TABLES=H5_1.1.1 BY S4
1366 /FORMAT=AVALUE TABLES
1367 /STATISTICS=CHISQ
1368 /CELLS=COUNT
1369 /COUNT ROUND CELL.
1370 CROSSTABS
1371 /TABLES=H5_1.1.1 BY S4
1372 /FORMAT=AVALUE TABLES
1373 /STATISTICS=CHISQ PHI
1374 /CELLS=COUNT EXPECTED
1375 /COUNT ROUND CELL.
1376 * Sec VS OPS BY Job Title [SIG.]*.
1377 CROSSTABS
1378 /TABLES=H5_1.1.1 BY S12
1379 /FORMAT=AVALUE TABLES
1380 /STATISTICS=CHISQ
1381 /CELLS=COUNT
1382 /COUNT ROUND CELL.
1383 * Sec VS OPS BY Educational Level *.
1384 CROSSTABS
1385 /TABLES=H5_1.1.1 BY S20.1
1386 /FORMAT=AVALUE TABLES
1387 /STATISTICS=CHISQ
1388 /CELLS=COUNT
1389 /COUNT ROUND CELL.
1390 * Sec VS OPS BY Annual Salary *.
1391 CROSSTABS
1392 /TABLES=H5_1.1.1 BY S17
1393 /FORMAT=AVALUE TABLES
1394 /STATISTICS=CHISQ
1395 /CELLS=COUNT
1396 /COUNT ROUND CELL.
1397 * Sec VS OPS BY Marital Status *.
```

A.1 Appendix: Experiment 1

```
1398 CROSSTABS
1399 /TABLES=H5_1.1.1 BY S21_1
1400 /FORMAT=AVALUE TABLES
1401 /STATISTICS=CHISQ
1402 /CELLS=COUNT
1403 /COUNT ROUND CELL.
1404 * Sec VS OPS BY Independent decisions *.
1405 CROSSTABS
1406 /TABLES=H5_1.1.1 BY S13
1407 /FORMAT=AVALUE TABLES
1408 /STATISTICS=CHISQ
1409 /CELLS=COUNT
1410 /COUNT ROUND CELL.
1411 * Sec VS OPS BY More CIA *.
1412 CROSSTABS
1413 /TABLES=H5_1.1.1 BY S14
1414 /FORMAT=AVALUE TABLES
1415 /STATISTICS=CHISQ
1416 /CELLS=COUNT
1417 /COUNT ROUND CELL.
1418 * Sec VS OPS BY Language *.
1419 CROSSTABS
1420 /TABLES=H5_1.1.1 BY S25
1421 /FORMAT=AVALUE TABLES
1422 /STATISTICS=CHISQ
1423 /CELLS=COUNT
1424 /COUNT ROUND CELL.
1425 * Sec VS OPS BY Who makes decisions*.
1426 CROSSTABS
1427 /TABLES=H5_1.1.1 BY S15
1428 /FORMAT=AVALUE TABLES
1429 /STATISTICS=CHISQ
1430 /CELLS=COUNT
1431 /COUNT ROUND CELL.
1432 * Sec VS OPS BY # of employees *.
1433 CROSSTABS
1434 /TABLES=H5_1.1.1 BY S16_1
1435 /FORMAT=AVALUE TABLES
1436 /STATISTICS=CHISQ
1437 /CELLS=COUNT
1438 /COUNT ROUND CELL.
1439
1440 *** F) Multiple Regressions ***.
1441 *** Multiple Regression Analysis *****.
1442 * SCATTERPLOTS for linearity requirement – first column: x=predictor & y=WTP*.
1443 * For the clearly exogenous vars, I use only AGE and (NUMBER OF) FAMILY DEPENDENTS *.
1444 * For GENERAL RISK *.
1445 * For Professional-related vars, I use YRS OF EXPERIENCE, YEARS IN CURRENT JOB, ... *.
1446
1447 * AGE against WTP *.
1448 GRAPH
1449 /SCATTERPLOT(MATRIX)=S18 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1450 /MISSING=LISTWISE.
1451 GRAPH
1452 /SCATTERPLOT(MATRIX)=S18 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1453 /MISSING=LISTWISE.
1454 * (NUMBER OF) FAMILY DEPENDENTS against WTP *.
```

A.1 Appendix: Experiment 1

```
1455 GRAPH
1456 /SCATTERPLOT(MATRIX)=S22_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1457 /MISSING=LISTWISE.
1458 GRAPH
1459 /SCATTERPLOT(MATRIX)=S22_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1460 /MISSING=LISTWISE.
1461 * GENERAL RISK against WTP *.
1462 GRAPH
1463 /SCATTERPLOT(MATRIX)=S5_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1464 /MISSING=LISTWISE.
1465 GRAPH
1466 /SCATTERPLOT(MATRIX)=S5_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1467 /MISSING=LISTWISE.
1468 * YEARS OF EXPERIENCE against WTP *.
1469 GRAPH
1470 /SCATTERPLOT(MATRIX)=S2_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1471 /MISSING=LISTWISE.
1472 GRAPH
1473 /SCATTERPLOT(MATRIX)=S2_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1474 /MISSING=LISTWISE.
1475 * YEARS IN CURRENT JOB against WTP *.
1476 GRAPH
1477 /SCATTERPLOT(MATRIX)=S3_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1478 /MISSING=LISTWISE.
1479 GRAPH
1480 /SCATTERPLOT(MATRIX)=S3_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1481 /MISSING=LISTWISE.
1482 * SEC-OPS TODAY against WTP *.
1483 GRAPH
1484 /SCATTERPLOT(MATRIX)=S8_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1485 /MISSING=LISTWISE.
1486 GRAPH
1487 /SCATTERPLOT(MATRIX)=S8_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1488 /MISSING=LISTWISE.
1489 * SEC CLOSE TO BUSINESS OBJECTIVES AT WORK against WTP *.
1490 GRAPH
1491 /SCATTERPLOT(MATRIX)=S9_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1492 /MISSING=LISTWISE.
1493 GRAPH
1494 /SCATTERPLOT(MATRIX)=S9_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1495 /MISSING=LISTWISE.
1496 * SEC CLOSE TO BUSINESS OBJECTIVES IN GENERAL against WTP *.
1497 GRAPH
1498 /SCATTERPLOT(MATRIX)=S10_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1499 /MISSING=LISTWISE.
1500 GRAPH
1501 /SCATTERPLOT(MATRIX)=S10_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1502 /MISSING=LISTWISE.
1503 * WILLINGNESS TO SACRIFICE SEC FOR SPEED against WTP *.
1504 GRAPH
1505 /SCATTERPLOT(MATRIX)=S11_1 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1506 /MISSING=LISTWISE.
1507 GRAPH
1508 /SCATTERPLOT(MATRIX)=S11_1 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1509 /MISSING=LISTWISE.
1510 * INCOME against WTP *.
1511 GRAPH
```

A.1 Appendix: Experiment 1

```
1512 /SCATTERPLOT(MATRIX)=S17 H1_1 H1_2 H1_3 H1_4 H1_5 H1_6 H1_7 H1_8
1513 /MISSING=LISTWISE.
1514 GRAPH
1515 /SCATTERPLOT(MATRIX)=S17 H1_9 H1_10 H1_11 H1_12 H2_6_1 H2_7_1 H2_8_1
1516 /MISSING=LISTWISE.
1517
1518 * BASIC REGRESSORS: clearly exogenous variables* (did not include Country & Nationality).
1519 * H1_1 *.
1520 REGRESSION
1521 /MISSING LISTWISE
1522 /STATISTICS COEFF OUTS R ANOVA
1523 /CRITERIA=PIN(.05) POUT(.10)
1524 /NOORIGIN
1525 /DEPENDENT H1_1
1526 /METHOD=BACKWARD S18 S19 S20_1 S21_1 S22_1 S25 PROFESSIONAL.
1527 REGRESSION
1528 /MISSING LISTWISE
1529 /STATISTICS COEFF OUTS R ANOVA
1530 /CRITERIA=PIN(.05) POUT(.10)
1531 /NOORIGIN
1532 /DEPENDENT H1_1
1533 /METHOD=ENTER Single Cohabiting Married Remarried Divorced Widowed Separated.
1534 REGRESSION
1535 /MISSING LISTWISE
1536 /STATISTICS COEFF OUTS R ANOVA
1537 /CRITERIA=PIN(.05) POUT(.10)
1538 /NOORIGIN
1539 /DEPENDENT H1_1
1540 /METHOD=ENTER Other SeniorExecutive ManagerialRole ITandSecurity ComplianceRisk.
1541
1542 REGRESSION
1543 /DESCRIPTIVES MEAN STDDEV CORR SIG N
1544 /MISSING LISTWISE
1545 /STATISTICS COEFF OUTS CI(95) R ANOVA COLLIN TOL CHANGE ZPP
1546 /CRITERIA=PIN(.05) POUT(.10)
1547 /NOORIGIN
1548 /DEPENDENT H1_1
1549 /METHOD=BACKWARD S18 S19 S20_1 S21_1 S22_1 S25 PROFESSIONAL
1550 /RESIDUALS DURBIN
1551 /CASEWISE PLOT(ZRESID) OUTLIERS(3).
1552 * the same with Zres x2 & all partial plots .
1553 REGRESSION
1554 /DESCRIPTIVES MEAN STDDEV CORR SIG N
1555 /MISSING LISTWISE
1556 /STATISTICS COEFF OUTS CI(95) BCOV R ANOVA COLLIN TOL CHANGE ZPP
1557 /CRITERIA=PIN(.05) POUT(.10)
1558 /NOORIGIN
1559 /DEPENDENT H1_7
1560 /METHOD=BACKWARD S18 S19 S20_1 S21_1 S22_1 S25
1561 /PARTIALPLOT ALL
1562 /SCATTERPLOT=(*ZRESID ,*ZPRED)
1563 /RESIDUALS DURBIN HISTOGRAM(ZRESID) NORMPROB(ZRESID)
1564 /CASEWISE PLOT(ZRESID) OUTLIERS(3).
1565 * with SAVE DIAGNOSTICS *.
1566 REGRESSION
1567 /DESCRIPTIVES MEAN STDDEV CORR SIG N
1568 /MISSING LISTWISE
```

A.1 Appendix: Experiment 1

```
1569 /STATISTICS COEFF OUTS CI(95) R ANOVA COLLIN TOL CHANGE ZPP
1570 /CRITERIA=PIN(.05) POUT(.10)
1571 /NOORIGIN
1572 /DEPENDENT H1_1
1573 /METHOD=ENTER S18 S19 S20_1 S21_1 S22_1 S25 S4
1574 /PARTIALPLOT ALL
1575 /SCATTERPLOT=(*ZRESID ,*ZPRED)
1576 /RESIDUALS DURBIN HISTOGRAM(ZRESID) NORMPROB(ZRESID)
1577 /CASEWISE PLOT(ZRESID) OUTLIERS(3)
1578 /SAVE PRED ZPRED ADJPRED MAHAL COOK LEVER ZRESID DRESID SDRESID SDBETA SDFIT
      COVRATIO.
1579 * with bootstrap*.
1580 BOOTSTRAP
1581 /SAMPLING METHOD=SIMPLE
1582 /VARIABLES TARGET=H1_1 INPUT= S19 S18_1 S20_1 S21_1 S22_1 S25
1583 /CRITERIA CILEVEL=95 CITYPE=BCA NSAMPLES=1000
1584 /MISSING USERMISSING=EXCLUDE.
1585 REGRESSION
1586 /MISSING LISTWISE
1587 /STATISTICS COEFF OUTS R ANOVA
1588 /CRITERIA=PIN(.05) POUT(.10)
1589 /NOORIGIN
1590 /DEPENDENT H1_1
1591 /METHOD=ENTER S19 S18_1 S20_1 S21_1 S22_1 S25.
1592 * The same with Marital Status (S21_1) transformed into different variables *.
1593 REGRESSION
1594 /DESCRIPTIVES MEAN STDDEV CORR SIG N
1595 /MISSING LISTWISE
1596 /STATISTICS COEFF OUTS CI(95) R ANOVA COLLIN TOL CHANGE ZPP
1597 /CRITERIA=PIN(.05) POUT(.10)
1598 /NOORIGIN
1599 /DEPENDENT H1_1
1600 /METHOD=BACKWARD S18 S19 S20_1 S22_1 S25 Cohabiting Married Remarried Separated Divorced
      Widowed
1601 /SCATTERPLOT=(*ZRESID ,*ZPRED)
1602 /RESIDUALS DURBIN
1603 /CASEWISE PLOT(ZRESID) OUTLIERS(3).
1604 * job title*.
1605 REGRESSION
1606 /DESCRIPTIVES MEAN STDDEV CORR SIG N
1607 /MISSING LISTWISE
1608 /STATISTICS COEFF OUTS CI(95) R ANOVA COLLIN TOL CHANGE ZPP
1609 /CRITERIA=PIN(.05) POUT(.10)
1610 /NOORIGIN
1611 /DEPENDENT H1_1
1612 /METHOD=BACKWARD S12
1613 /RESIDUALS DURBIN
1614 /CASEWISE PLOT(ZRESID) OUTLIERS(3).
1615 * Basic regressors (+) RISK S5_1*.
1616 REGRESSION
1617 /DESCRIPTIVES MEAN STDDEV CORR SIG N
1618 /MISSING LISTWISE
1619 /STATISTICS COEFF OUTS CI(95) R ANOVA COLLIN TOL CHANGE ZPP
1620 /CRITERIA=PIN(.05) POUT(.10)
1621 /NOORIGIN
1622 /DEPENDENT H1_8
1623 /METHOD=BACKWARD S18 S19 S20_1 S21_1 S22_1 S25 S1 S5_1
```

A.1 Appendix: Experiment 1

```
1624 /RESIDUALS DURBIN
1625 /CASEWISE PLOT(ZRESID) OUTLIERS(3).
1626 * MODERATION EFFECTS: use PROFESSIONAL var as a moderator*.
1627 REGRESSION
1628 /MISSING LISTWISE
1629 /STATISTICS COEFF OUTS CI(95) R ANOVA COLLIN TOL CHANGE
1630 /CRITERIA=PIN(.05) POUT(.10)
1631 /NOORIGIN
1632 /DEPENDENT H1_1
1633 /METHOD=ENTER S19
1634 /METHOD=ENTER S18
1635 /SAVE PRED COOK LEVER SRESID SDRESID.
1636
1637 * Chart Builder – remember to remove SPLIT by S1 !.
1638 GGRAPH
1639 /GRAPHDATASET NAME="graphdataset" VARIABLES=MEANCI(RiskAversionH1_1, 95) MEANCI(
1640 RiskAversionH1_2,
1641 95) MEANCI(RiskAversionH1_3, 95) MEANCI(RiskAversionH1_4, 95) MEANCI(RiskAversionH1_5, 95)
1642 MEANCI(RiskAversionH1_6, 95) MEANCI(RiskAversionH1_7, 95) MEANCI(RiskAversionH1_8, 95)
1643 MEANCI(RiskAversionH1_9, 95) MEANCI(RiskAversionH1_10, 95) MEANCI(RiskAversionH1_11, 95)
1644 MEANCI(RiskAversionH1_12, 95) S1 MISSING=LISTWISE REPORTMISSING=NO
1645 TRANSFORM=VARSTOCASES(SUMMARY="#SUMMARY" INDEX="#INDEX" LOW="#LOW" HIGH="#
HIGH")
1646 /GRAPHSPEC SOURCE=INLINE.
1647 BEGIN GPL
1648 SOURCE: s=userSource(id("graphdataset"))
1649 DATA: SUMMARY=col(source(s), name("#SUMMARY"))
1650 DATA: INDEX=col(source(s), name("#INDEX"), unit.category())
1651 DATA: S1=col(source(s), name("S1"), unit.category())
1652 DATA: LOW=col(source(s), name("#LOW"))
1653 DATA: HIGH=col(source(s), name("#HIGH"))
1654 COORD: rect(dim(1,2), cluster(3,0))
1655 GUIDE: axis(dim(2), label("Mean"))
1656 GUIDE: legend(aesthetic(aesthetic.color.interior), label("Are you (or have you been) related ",
1657 "to the profession or practice of Information Security in any way?"))
1658 GUIDE: text.footnote(label("Error Bars: 95% CI"))
1659 SCALE: cat(dim(3), include("0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11"))
1660 SCALE: linear(dim(2), include(0))
1661 SCALE: cat(aesthetic(aesthetic.color.interior), include("1", "2"))
1662 SCALE: cat(dim(1), include("1", "2"))
1663 ELEMENT: interval(position(S1*SUMMARY*INDEX), color.interior(S1), shape.interior(shape.square))
1664 ELEMENT: interval(position(region.spread.range(S1*(LOW+HIGH)*INDEX)), shape.interior(shape.ibeam))
1665 END GPL.
```

A.1.14 Linear Models Regression Specifications

Experiment 1: Specifications

We conducted a number of regressions with bootstrapping on all survey variables, by the following specifications. In the initial three regression models the dependent variable is willingness to pay (WTP), i.e. the series H_1i and variables $H_26,7$ and 8.

Specification 1: explores potential differences between the population of professionals and the students sample. The predictors used in the model are the clearly exogenous variables.

Dependent variable: all variables of Table A.1 (H1 Instrument) and variables $H_26,7$ and 8.

Predictors: age, gender, education, marital status, number of dependents in family, country, nationality, language.

Sample: professionals and students.

Specification 2: is the same as Specification 1, having only the additional variable of general risk ('How willing are you to take risks in general?').

Specification 3: aims to explore potential differences amongst the population of professionals. The predictors used in the model are related to information security.

Dependent variable: all variables of Table A.1 (H1 Instrument) along with variables $H_26,7$ and 8.

Predictors: years of experience, years in current job position, experience of security incident, security-operations tradeoff today, closeness of security to business objectives today, closeness of security to business objectives in job environment, willingness to sacrifice security for speed of operations, job title, need for more confidentiality, integrity and availability measures in job environment, person who makes security decisions at work, salary, power to make independent security decisions at work.

Sample: professionals.

Specification 4: is different from the first three specifications. In this case, we considered WTP as fixed preference and we explored the influence of the expressed 'worry' of the subjects on WTP.

Dependent variable: worry about security incidents at work and worry about new unidentified security threats.

Predictors: age, gender, education, marital status, number of dependents in family, language.

Sample: professionals and students.

A.1 Appendix: Experiment 1

A.1.15 Definitions

Experiment 1: Definitions

H_{xy} :	A lottery with index y , that is mainly related to hypothesis x .
H_{11} to H_{12} :	Two-outcome lotteries with negative or zero outcomes; participants stated their willingness to pay to avoid these lotteries.
H_{21} to H_{25} :	Variables that describe comparisons of pairs of L_i lotteries.
H_{26} to H_{28} :	Five-outcome lotteries with large losses; participants stated their willingness to pay to avoid these lotteries.
L_i :	Various five-outcome lotteries used in lottery comparisons.
Group A:	Lotteries H_{11} to H_{14} with expected value $\mu = -2.5$.
Group B:	Lotteries H_{15} to H_{18} with expected value $\mu = -7.5$.
Group C:	Lotteries H_{19} to H_{12} with expected value $\mu = -25$.
Scenario1:	Experiment question in which participants chose between enhancement of either security or operability.
Scenario2:	Experiment mechanism in which participants chose between: A) remaining in the current system state, B) enhancement and reduction of security and operability (based on previous answers) and C) indifference between A and B.
$SWITCHPOINT_SEC$:	Variable that denotes a switching point of enhancing security by $x\%$ and operability by 10%, after which, operability enhancement became more attractive to the subject.
$SWITCHPOINT_OPS$:	Variable that denotes a switching point of enhancing operability by $x\%$ and security by 10%, after which, security enhancement became more attractive to the subject.
$LOSS_AV_SEC$:	Variable that measures the difference between $SWITCHPOINT_SEC$ and elicited preferences of Scenario 2.
$LOSS_AV_OPS$:	Variable that measures the difference between $SWITCHPOINT_OPS$ and elicited preferences of Scenario 2.
$RiskAversionHx_y$:	Variable that measures the difference between participants' WTP and the expected value of lottery H_{xy} .

A.2 Appendix: Experiment 2

A.2.1 Experiment Design

A.2.1.1 All Experiment and Survey Lotteries

Group A

GroupA L1 Lottery1: There is a 5% probability of losing \$10 and a 95% probability of losing \$0. Your current amount is \$30.

GroupA L1A Situation 1: What is the maximum amount that you are willing to pay in order to reduce probability of loss from 5% to 2.5%?

GroupA L1B Situation 2: What is the maximum amount that you are willing to pay in order to reduce potential loss from \$10 to \$5?

GroupA L1C Situation 3: What is the maximum amount that you are willing to pay in order to avoid playing the lottery completely?

GroupA L2 Lottery2: There is a 15% probability of losing \$10 and an 85% probability of losing \$0. Your current amount is \$30.

GroupA L2A Situation 1: What is the maximum amount that you are willing to pay in order to reduce probability of loss from 15% to 7.5%?

GroupA L2B Situation 2: What is the maximum amount that you are willing to pay in order to reduce potential loss from \$10 to \$5?

GroupA L2C Situation 3: What is the maximum amount that you are willing to pay in order to avoid playing the lottery completely?

GroupA L3 Lottery3: There is a 50% probability of losing \$10 and a 50% probability of losing \$0. Your current amount is \$30.

GroupA L3A Situation 1: What is the maximum amount that you are willing to pay in order to reduce probability of loss from 50% to 25%?

GroupA L3B Situation 2: What is the maximum amount that you are willing to pay in order to reduce potential loss from \$10 to \$5?

GroupA L3C Situation 3: What is the maximum amount that you are willing to pay in order to avoid playing the lottery completely?

A.2 Appendix: Experiment 2

GroupB

GroupB L1 Lottery1: There is a 95% probability of gaining \$10 and a 5% probability of gaining \$0. Your current amount is \$0.

GroupB L1A Situation 1: What is the maximum amount that you are willing to pay in order to increase probability of gaining from 95% to 97.5%?

GroupB L1B Situation 2: What is the maximum amount that you are willing to pay in order to increase the potential outcome of gaining nothing to gaining \$5?

GroupB L1C Situation 3: What is the maximum amount that you are willing to pay in order to avoid the lottery risk and gain \$10 for sure?

GroupB L2 Lottery2: There is an 85% probability of gaining \$10 and a 15% probability of gaining \$0. Your current amount is \$0.

GroupB L2A Situation 1: What is the maximum amount that you are willing to pay in order to increase probability of gaining from 85% to 92.5%?

GroupB L2B Situation 2: What is the maximum amount that you are willing to pay in order to increase the potential outcome of gaining nothing to gaining \$5?

GroupB L2C Situation 3: What is the maximum amount that you are willing to pay in order to avoid the lottery risk and gain \$10 for sure?

GroupB L3 Lottery3: There is a 50% probability of gaining \$10 and a 50% probability of gaining \$0. Your current amount is \$0.

GroupB L3A Situation 1: What is the maximum amount that you are willing to pay in order to increase probability of gaining from 50% to 75%?

GroupB L3B Situation 2: What is the maximum amount that you are willing to pay in order to increase the potential outcome of gaining nothing to gaining \$5?

GroupB L3C Situation 3: What is the maximum amount that you are willing to pay in order to avoid the lottery risk and gain \$10 for sure?

A.2 Appendix: Experiment 2

Group C

GroupC L1 You are given \$10 to play Lottery1: There is a 5% probability of losing \$10 and a 95% probability of losing \$0.

GroupC L1A Situation 1: What is the maximum amount that you are willing to pay in order to reduce probability of loss from 5% to 2.5%?

GroupC L1B Situation 2: What is the maximum amount that you are willing to pay in order to reduce potential loss from \$10 to \$5?

GroupC L1C Situation 3: What is the maximum amount that you are willing to pay in order to completely avoid the risk of losing \$10?

GroupC L2 You are given \$10 to play Lottery2: There is a 15% probability of losing \$10 and an 85% probability of losing \$0.

GroupC L2A Situation 1: What is the maximum amount that you are willing to pay in order to reduce probability of loss from 15% to 7.5%?

GroupC L2B Situation 2: What is the maximum amount that you are willing to pay in order to reduce potential loss from \$10 to \$5?

GroupC L2C Situation 3: What is the maximum amount that you are willing to pay in order to completely avoid the risk of losing \$10?

GroupC L3 You are given \$10 to play Lottery3: There is a 50% probability of losing \$10 and a 50% probability of losing \$0.

GroupC L3A Situation 1: What is the maximum amount that you are willing to pay in order to reduce probability of loss from 50% to 25%?

GroupC L3B Situation 2: What is the maximum amount that you are willing to pay in order to reduce potential loss from \$10 to \$5?

GroupC L3C Situation 3: What is the maximum amount that you are willing to pay in order to completely avoid the risk of losing \$10?

A.2 Appendix: Experiment 2

Payment Lottery:

All lotteries beneath have non-negative potential outcomes. Which of the following lotteries do you prefer to play?

- A) There is a 50% probability of gaining 0\$ and a 50% probability of gaining \$10.
- B) There is a 50% probability of gaining 2\$ and a 50% probability of gaining \$8.
- C) There is a 50% probability of gaining 4\$ and a 50% probability of gaining \$6.

Common-for-all-participants Lotteries:

L1 There is a 5% probability of losing \$50 and a 95% probability of losing \$0.

L1A What is the maximum amount that you are willing to pay in order to reduce probability of loss from 5% to 2.5%?

L1B What is the maximum amount that you are willing to pay in order to reduce potential loss from \$50 to \$25?

L1C What is the maximum amount that you are willing to pay in order to avoid playing the lottery completely?

L2 There is a 15% probability of losing \$50 and an 85% probability of losing \$0.

L2A What is the maximum amount that you are willing to pay in order to reduce probability of loss from 15% to 7.5%?

L2B What is the maximum amount that you are willing to pay in order to reduce potential loss from \$50 to \$25?

L2C What is the maximum amount that you are willing to pay in order to avoid playing the lottery completely?

L3 There is a 50% probability of losing \$50 and a 50% probability of losing \$0.

L3A What is the maximum amount that you are willing to pay in order to reduce probability of loss from 50% to 25%?

L3B What is the maximum amount that you are willing to pay in order to reduce potential loss from \$50 to \$25?

L3C What is the maximum amount that you are willing to pay in order to avoid playing the lottery completely?

A.2 Appendix: Experiment 2

Common-for-all-participants Survey-Lotteries:

SL1 You need to protect an asset that is worth \$ 75,000. There is a 5% probability that a (confidentiality/integrity/availability) threat will materialise.

SL1A What is the maximum amount that you are willing to pay in order to reduce probability of loss from 5% to 2.5%?

SL1B What is the maximum amount that you are willing to pay in order to reduce potential asset loss from \$75,000 to \$37,500?

SL1C What is the maximum amount that you are willing to pay in order to avoid the risk completely?

SL2 You need to protect an asset that is worth \$ 75,000. There is a 15% probability that a (confidentiality/integrity/availability) threat will materialise.

SL2A What is the maximum amount that you are willing to pay in order to reduce probability of loss from 15% to 7.5%?

SL2B What is the maximum amount that you are willing to pay in order to reduce potential asset loss from \$75,000 to \$37,500?

SL2C What is the maximum amount that you are willing to pay in order to avoid the risk completely?

SL3 You need to protect an asset that is worth \$ 75,000. There is a 50% probability that a (confidentiality/integrity/availability) threat will materialise.

SL3A What is the maximum amount that you are willing to pay in order to reduce probability of loss from 50% to 25%?

SL3B What is the maximum amount that you are willing to pay in order to reduce potential asset loss from \$75,000 to \$37,500?

SL3C What is the maximum amount that you are willing to pay in order to avoid the risk completely?

A.2 Appendix: Experiment 2

A.2.1.2 Consent Form

Experiment 2: Consent Form

Thank you for taking part in this experiment and survey!

Your participation is very helpful for my cross-disciplinary PhD research in the Information Security Group and Economics Department at Royal Holloway University of London.

Konstantinos

Procedure:

You will be asked to make decisions about lotteries and fill out a survey with information security related questions and demographics. Duration is no more than about 20 minutes.

Benefits and Scope of this Study:

By completing this questionnaire, you have the opportunity to win up to \$10.

At the end of the experiment, one of the lotteries in the questionnaire will be 'executed' by the computer. Your payment will be based on your choices in this lottery and the random draw of the computer. An email will be sent to your designated email address with your payment in the form of an Amazon gift certificate.

Please, note that for the payment to be processed, it is necessary that you do not just answer randomly and instead make all your decisions carefully.

Your participation will allow us to collect valuable data for our research.

Confidentiality:

No identification of the participants is collected or maintained during or after the completion of the experiment and the survey and all data are fully anonymised. An email address is requested at the end of the survey only for the purpose of sending your payment. All data will be protected and kept completely confidential.

Usage of the findings:

The research findings will be used for academic purposes only. For example, they might be presented in academic conferences, and be published in research journals in the field of Information Security and Economics. Research findings will be made available to all participants upon request after data collection and data analysis.

Contact information:

In case of any concern or question, please contact Konstantinos at:

konstantinos.mersinas.2011@rhul.ac.uk or call directly at +44... .

By beginning the survey you acknowledge that you have read this form and agree to participate in this research.

A.2 Appendix: Experiment 2

A.2.1.3 Survey Questions

Question: “Are you related with the profession or practice of Information Security in any way?”

Question: ‘What is your gender?’

Question: ‘What is your age?’

Question: “What is your educational level?”

Question: “What is your marital status?”

Question: “What is the number of dependants in your family?”

Question: “What is your approximate annual income in US dollars?”

Question: “Approximately how many employees work in your company / organisation?”

Question: “How willing are you to take risks in general?”

Question: “Your job title most closely resembles:”

- *Senior executive role (e.g. CEO, CIO, CISO, CSO etc.)*
- *Managerial role (e.g. Project Manager, IT Director, Security Manager etc.)*
- *IT & Security (e.g. Security Officer, System Administrator, Information Analyst etc.)*
- *Compliance, Risk or Privacy role (e.g. Consultant, Auditor etc.)*
- *Other: please specify*

A.2 Appendix: Experiment 2

Question: “How many years of experience do you have in Information Security related tasks?”

Question: “How long have you held your current job position for?”

Question: “An information security incident is made up of one or more unwanted or unexpected information security events that could compromise security and weaken or impair business operations.

An information security event implies that the security of a system, service, or network has been breached, indicating that a security policy has been violated or a safeguard has failed.

Have you experienced any critical or worth-mentioning information security incidents?”

Question: “Do you feel that your company / organisation needs to take more actions for protecting confidentiality, integrity or availability?”

Question: “Do you feel that your job position allows you to make independent security related decisions?”

Question: “How worried are you about new unidentified information security threats?”

Question: “Is English your mother tongue?”

Question: “Which Amazon website do you prefer for your gift certificate payment?

(payment amount will be converted from US Dollars to the corresponding currency if needed)”

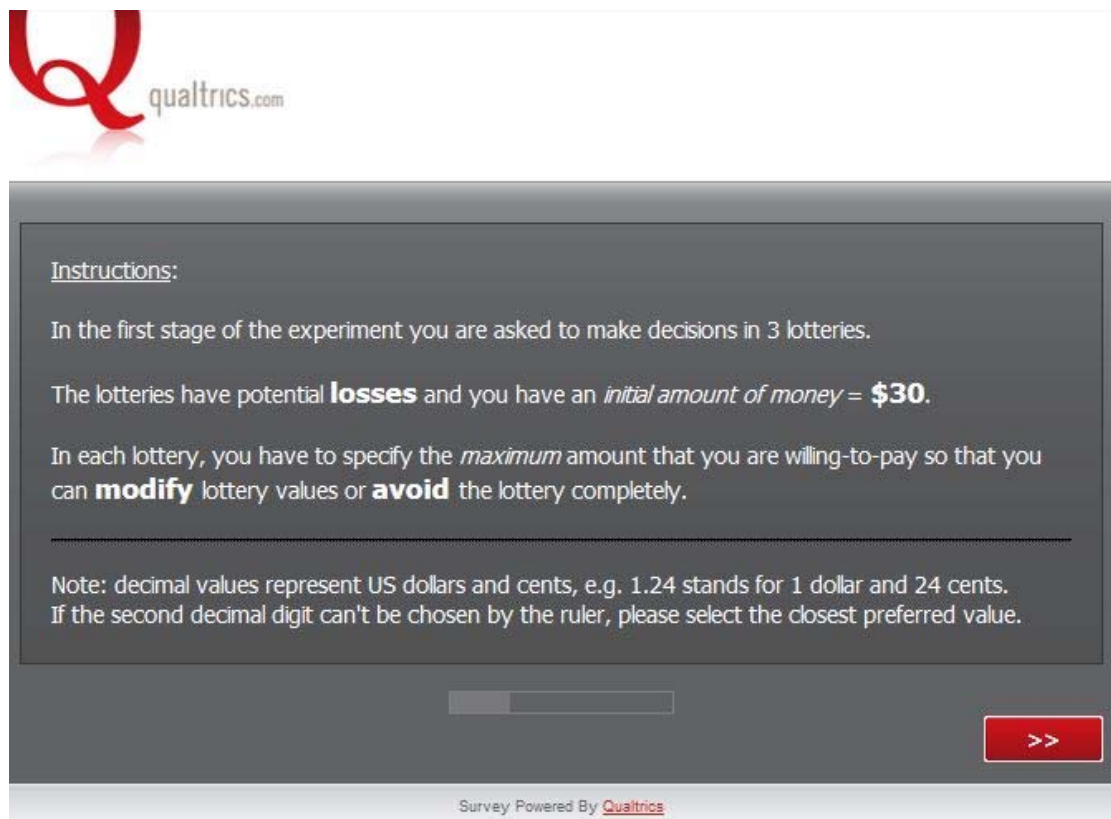
A.2 Appendix: Experiment 2

Question: “Please, enter your email address:
(this is to be used only for sending you an Amazon gift certificate code)”

Note: Likert-scale questions presented participants with a bar, valued from 1 to 10, e.g. “0: *Not worried at all* 10: *Very worried*”.

A.2.2 Experiment 2 Indicative Screenshots

Figure A.12: In the beginning of the experiment participants are randomly placed into one of the three treatment groups (here we have the “Losses frame group”).



A.2 Appendix: Experiment 2

Figure A.13: Indicative lotteries that participants have to make risk decisions on.

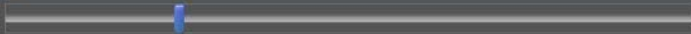
Lottery3: There is a **50%** probability of losing **\$10** and a **50%** probability of losing **\$0**.

Your current amount is **\$30**

Situation 1: What is the maximum amount that you are willing to pay in order to reduce probability of loss from **50%** to **25%** ?

0 1 2 3 4 5 6 7 8 9 10


\$



Situation 2: What is the maximum amount that you are willing to pay in order to reduce potential loss from **\$10** to **\$5** ?

0 1 2 3 4 5 6 7 8 9 10

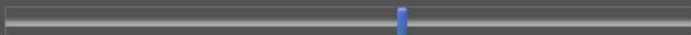
\$



Situation 3: What is the maximum amount that you are willing to pay in order to **avoid** playing the lottery completely?

0 1 2 3 4 5 6 7 8 9 10

\$



>>

Figure A.14: Participants are presented with the lottery that will produce their payment, without knowing it.

All lotteries beneath have non-negative potential outcomes.

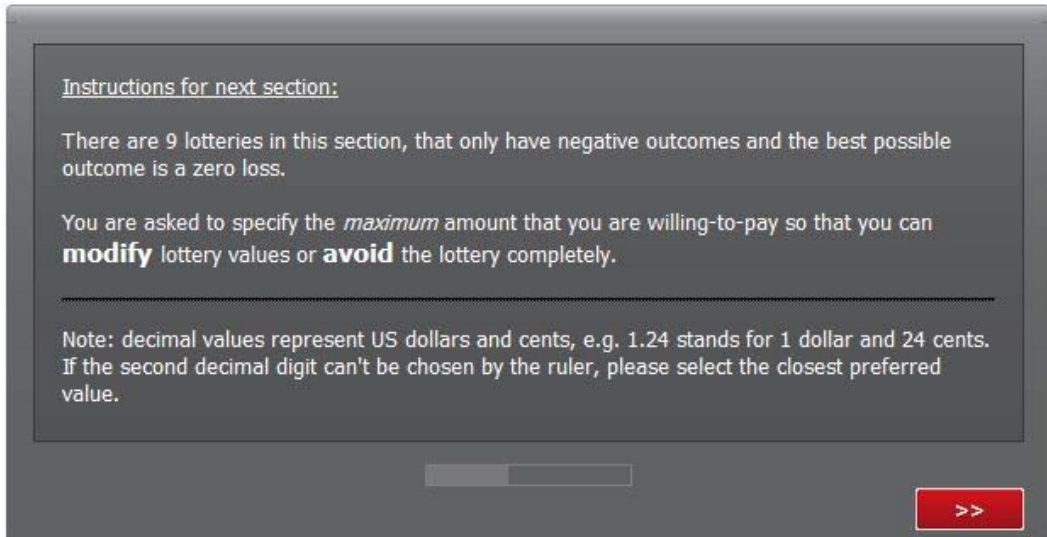
Which of the following lotteries do you prefer to play?

- A) There is a **50%** probability of gaining **0\$** and a **50%** probability of gaining **\$10**.
- B) There is a **50%** probability of gaining **2\$** and a **50%** probability of gaining **\$8**.
- C) There is a **50%** probability of gaining **4\$** and a **50%** probability of gaining **\$6**.

>>

A.2 Appendix: Experiment 2

Figure A.15: Instructions given for the second part of the experiment.



Instructions for next section:

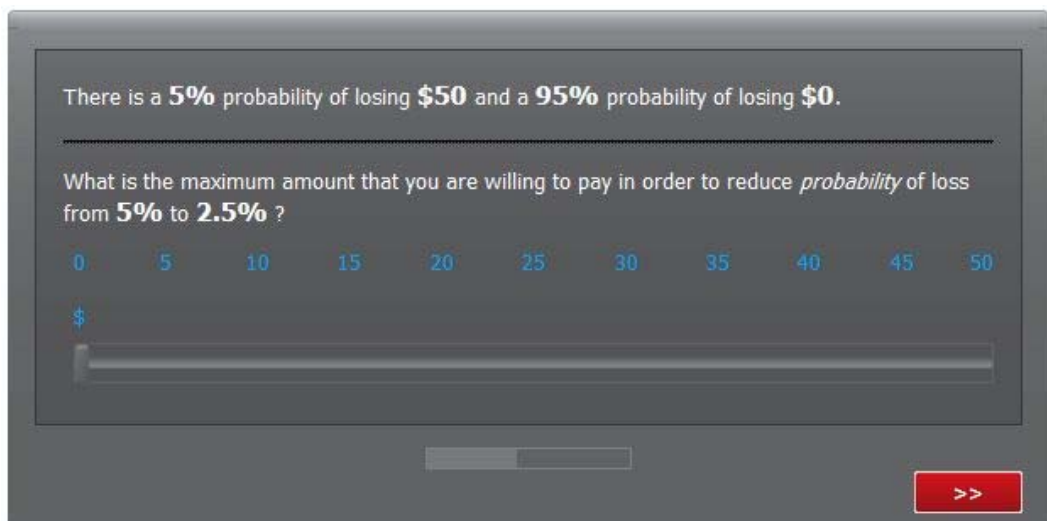
There are 9 lotteries in this section, that only have negative outcomes and the best possible outcome is a zero loss.

You are asked to specify the *maximum* amount that you are willing-to-pay so that you can **modify** lottery values or **avoid** the lottery completely.

Note: decimal values represent US dollars and cents, e.g. 1.24 stands for 1 dollar and 24 cents. If the second decimal digit can't be chosen by the ruler, please select the closest preferred value.

>>

Figure A.16: WTP for probability reduction.



There is a **5%** probability of losing **\$50** and a **95%** probability of losing **\$0**.

What is the maximum amount that you are willing to pay in order to reduce *probability* of loss from **5%** to **2.5%** ?

0 5 10 15 20 25 30 35 40 45 50

\$

>>

A.2 Appendix: Experiment 2

Figure A.17: WTP for loss reduction.

There is a **15%** probability of losing **\$50** and an **85%** probability of losing **\$0**.

What is the maximum amount that you are willing to pay in order to reduce potential *loss* from **\$50** to **\$25** ?

0 5 10 15 20 25 30 35 40 45 50

\$

A horizontal slider bar is shown below the numbers, with a blue vertical marker positioned at the value 5. Below the slider is a progress indicator and a red button with the text '>>'.

Figure A.18: WTP for avoiding the lottery completely.

There is a **15%** probability of losing **\$50** and an **85%** probability of losing **\$0**.

What is the maximum amount that you are willing to pay in order to **avoid** playing the lottery completely?

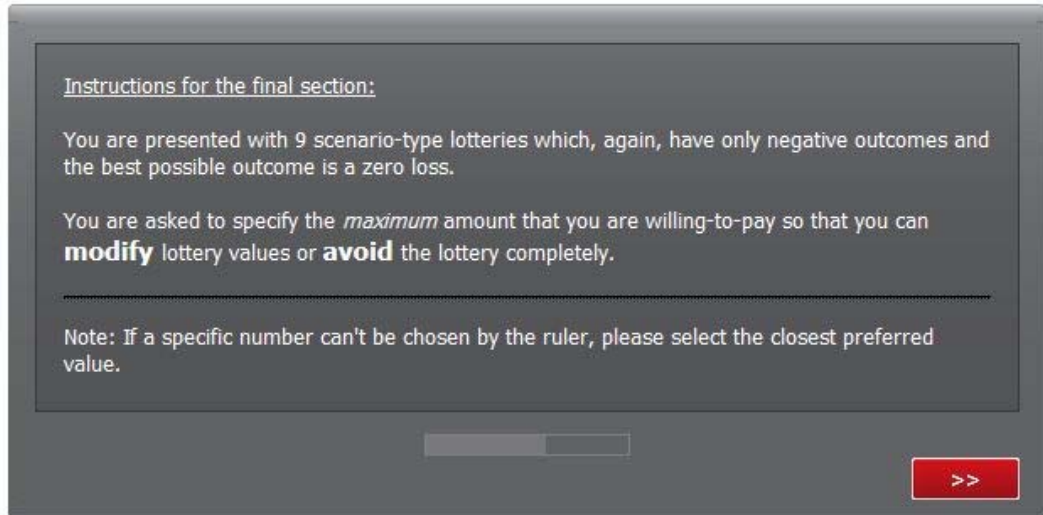
0 5 10 15 20 25 30 35 40 45 50

\$

A horizontal slider bar is shown below the numbers, with a blue vertical marker positioned at the value 10. Below the slider is a progress indicator and a red button with the text '>>'.

A.2 Appendix: Experiment 2

Figure A.19: Instructions for the final part of the experiment.



Instructions for the final section:

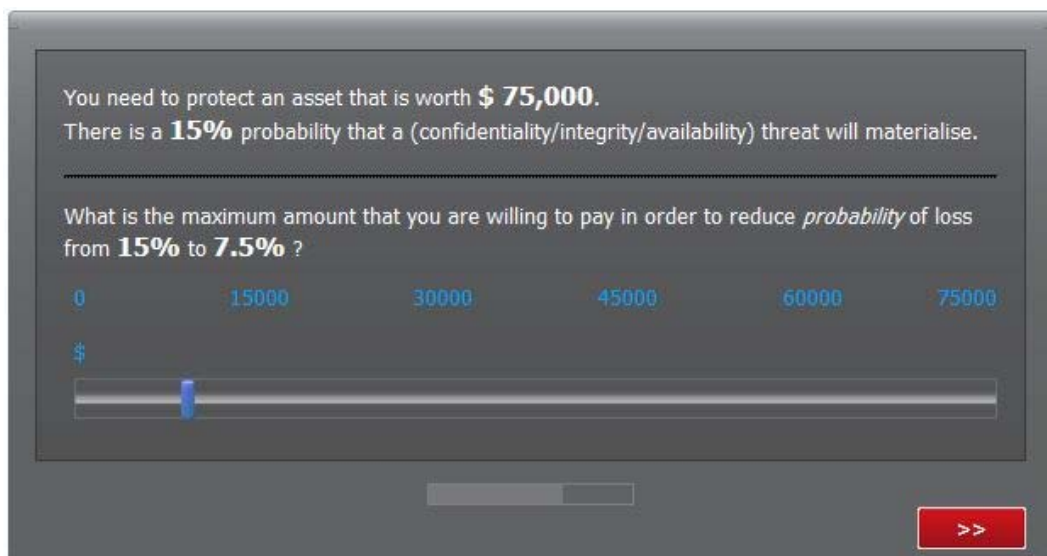
You are presented with 9 scenario-type lotteries which, again, have only negative outcomes and the best possible outcome is a zero loss.

You are asked to specify the *maximum* amount that you are willing-to-pay so that you can **modify** lottery values or **avoid** the lottery completely.

Note: If a specific number can't be chosen by the ruler, please select the closest preferred value.

>>

Figure A.20: WTP for probability reduction in a scenario.



You need to protect an asset that is worth **\$ 75,000**.
There is a **15%** probability that a (confidentiality/integrity/availability) threat will materialise.

What is the maximum amount that you are willing to pay in order to reduce *probability* of loss from **15%** to **7.5%** ?

0 15000 30000 45000 60000 75000

\$

>>

A.2 Appendix: Experiment 2

Figure A.21: WTP for loss reduction in a scenario.

You need to protect an asset that is worth **\$ 75,000**.
There is a **15%** probability that a (confidentiality/integrity/availability) threat will materialise.

What is the maximum amount that you are willing to pay in order to reduce potential asset *loss* from **\$75,000** to **\$37,500** ?

0 15000 30000 45000 60000 75000

\$

Slider bar with a blue marker at approximately 15,000.

Next button (red with >>)

Figure A.22: WTP for avoiding the lottery completely in a scenario.

You need to protect an asset that is worth **\$ 75,000**.
There is a **15%** probability that a (confidentiality/integrity/availability) threat will materialise.

What is the maximum amount that you are willing to pay in order to **avoid** the risk completely?

0 15000 30000 45000 60000 75000

\$

Slider bar with a blue marker at approximately 15,000.

Next button (red with >>)

A.2 Appendix: Experiment 2

Figure A.23: Information given regarding the payment method.

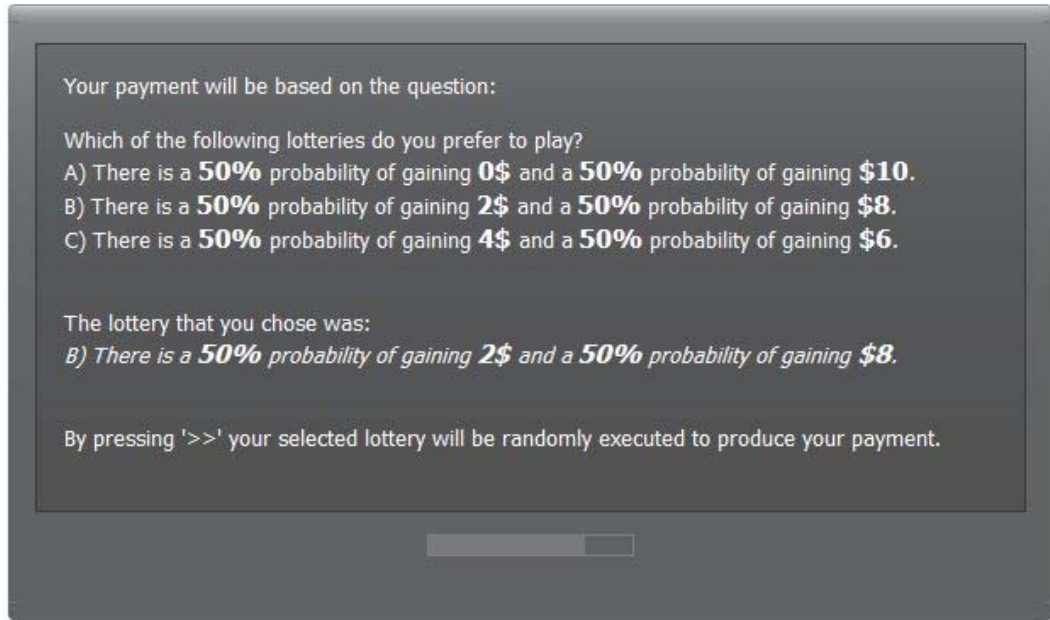


Figure A.24: An indicative payment message.



A.2 Appendix: Experiment 2

Figure A.25: Demographics and survey.

You have reached the final survey page. All information provided will be kept **confidential**.

Are you (or have you been) related to the profession or practice of Information Security in any way?

Yes
 No

What is your gender?

Male
 Female

What is your age?

age

What is your educational level?

education

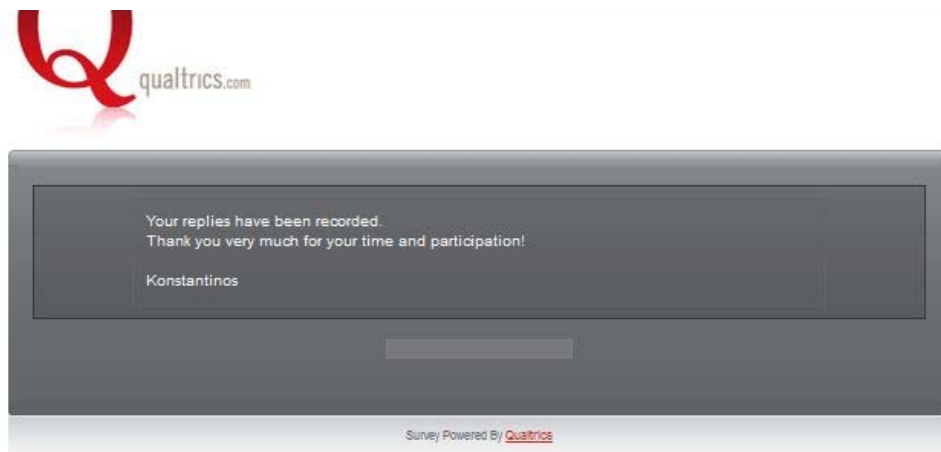
What is your marital status?

marital status

What is the number of dependants in your family?

number of dependants

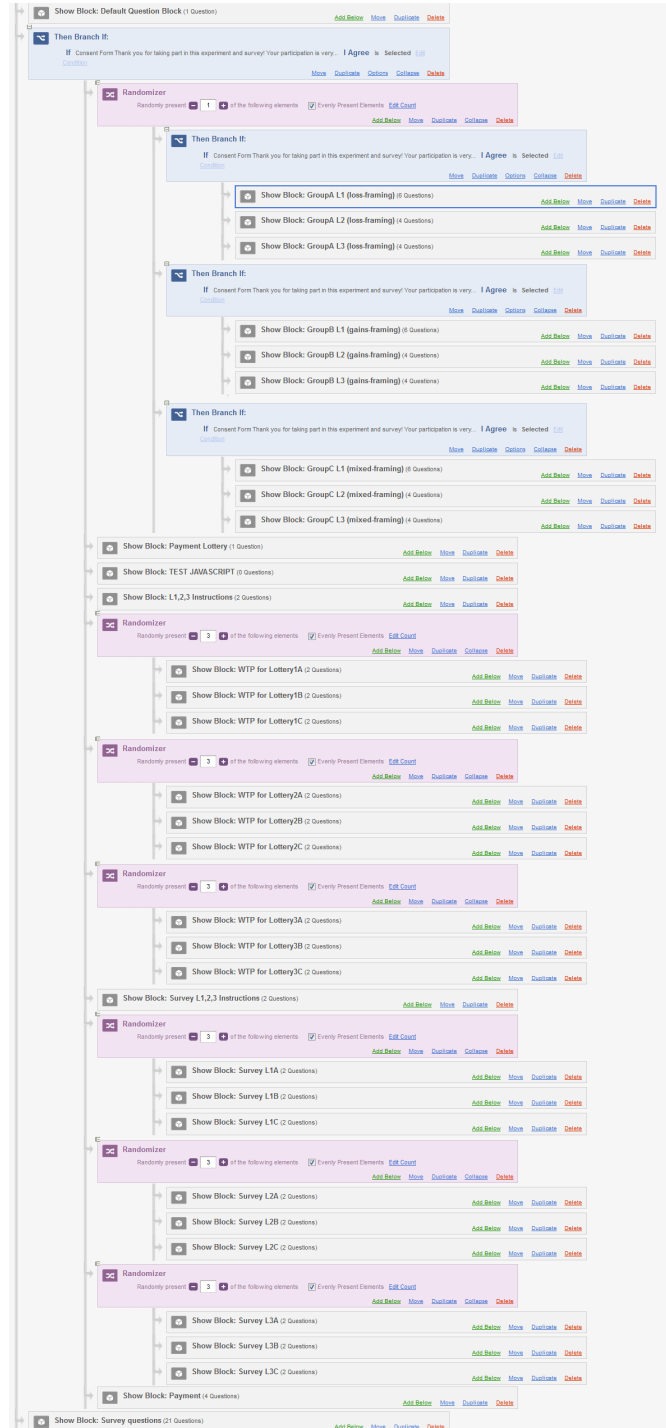
Figure A.26: End message.



A.2 Appendix: Experiment 2

A.2.2.1 Experiment Flow

Figure A.27: Experiment Flow (Qualtrics Software [3]).



A.2 Appendix: Experiment 2

A.2.3 Definitions

Experiment 2: Definitions

L_{ij} :	lottery $i = 1, 2$ or 3 and subquestion $j = A, B$ or C . Subquestion A refers to reduction of probability, B to reduction of outcome and C corresponds to risk elimination.
SL_{ij} :	the same as above, for survey lotteries.
$L_{iC-half}, SL_{iC-half}$:	halved WTP values for eliminating risk (not playing the lottery) lotteries, $i = 1, 2$ or 3 .
$Groups$:	these are the three conditions that randomly assign participants to the framing of (A) gains, (B) losses and (C) mixed gains and losses.
$Group_k-L_{ij}$:	lottery $i = 1, 2$ or 3 , subquestion $j = A, B$ or C for the framing group $k = A, B$ or C . The unified variable for the three groups is called $Groups-L_{ij}$ and is used in the analysis in conjunction with a group-indicating variable.
$Delta_EV_lottery$:	for each lottery, the “delta expected value” is the difference between the expected value of the original lottery and the expected value of the proposed modified lottery.
$RA_lottery$:	for each lottery, the “risk aversion variable” represents participant’s elicited WTP minus $Delta_EV_lottery$. For example, if $WTP > Delta_EV_$ for some lottery, this means that the subject is willing to pay more than the objective reduction of the expected value between the original and the modified lottery, and therefore the subject is risk averse.

A.2 Appendix: Experiment 2

A.2.4 Qualtrics Javascript Code

```
1 Qualtrics.SurveyEngine.addOnload(function()  
2 {  
3   var ambig03to10 = Math.random()*0.7+0.3;  
4   var ambig03to08 = Math.random()*0.5+0.3;  
5   var ambig04to06 = Math.random()*0.2+0.4;  
6   var payA = ambig03to10*10;  
7   var payB = ambig03to08*10;  
8   var payC = ambig04to06*10;  
9   var paymentA = Math.round(payA/100)*100;  
10  var paymentB = Math.round(payB/100)*100;  
11  var paymentC = Math.round(payC/100)*100;  
12  
13  
14  Qualtrics.SurveyEngine.setEmbeddedData('Ambig03to10', ambig03to10);  
15  Qualtrics.SurveyEngine.setEmbeddedData('Ambig03to08', ambig03to08);  
16  Qualtrics.SurveyEngine.setEmbeddedData('Ambig04to06', ambig04to06);  
17  Qualtrics.SurveyEngine.setEmbeddedData('PaymentA', paymentA);  
18  Qualtrics.SurveyEngine.setEmbeddedData('PaymentB', paymentB);  
19  Qualtrics.SurveyEngine.setEmbeddedData('PaymentC', paymentC);  
20  
21  
22  this.hideNextButton();  
23  this.showNextButton.delay(6);  
24  
25 });
```

A.2 Appendix: Experiment 2

A.2.5 Experiment Analysis

A.2.6 SPSS Syntax Code

The following code includes data cleaning and analysis in SPSS version 21 [1].

```
1  *ï***** DATASETS *****.
2  *** Copy all finalised cases into a new DataSet called 'Exp2_Finalised' ***.
3  DATASET ACTIVATE DataSet1.
4  DATASET COPY Exp2_Finalised.
5  DATASET ACTIVATE Exp2_Finalised.
6  FILTER OFF.
7  USE ALL.
8  SELECT IF (NOT(V10=0)).
9  EXECUTE.
10
11 *** Now, run code on the new DataSet ***.
12 ***** VARIABLES *****.
13 *** Convert all Embedded Data variables (STRINGS) to F Format, with 2 decimals ***.
14 alter type GA_L1A GA_L1B GA_L1C GB_L1A GB_L1B GB_L1C GC_L1A GC_L1B GC_L1C (f2).
15 alter type GA_L2A GA_L2B GA_L2C GB_L2A GB_L2B GB_L2C GC_L2A GC_L2B GC_L2C (f2).
16 alter type GA_L3A GA_L3B GA_L3C GB_L3A GB_L3B GB_L3C GC_L3A GC_L3B GC_L3C (f2).
17 alter type SL1A SL1B SL1C SL2A SL2B SL2C SL3A SL3B SL3C (f2).
18 alter type L1A L1B L1C L2A L2B L2C L3A L3B L3C (f2).
19 VARIABLE LEVEL L1A L1B L1C L2A L2B L2C L3A L3B L3C (SCALE).
20 VARIABLE LEVEL GA_L1A GA_L1B GA_L1C GB_L1A GB_L1B GB_L1C GC_L1A GC_L1B GC_L1C (SCALE).
21 VARIABLE LEVEL GA_L2A GA_L2B GA_L2C GB_L2A GB_L2B GB_L2C GC_L2A GC_L2B GC_L2C (SCALE).
22 VARIABLE LEVEL GA_L3A GA_L3B GA_L3C GB_L3A GB_L3B GB_L3C GC_L3A GC_L3B GC_L3C (SCALE).
23 VARIABLE LEVEL SL1A SL1B SL1C SL2A SL2B SL2C SL3A SL3B SL3C (SCALE).
24 VARIABLE LEVEL Incident Indep English Job Marital Gender Protect (NOMINAL).
25 VARIABLE LEVEL Income Employees Edu Worried PaymentLottery (ORDINAL).
26
27 * Calculate half of the values of WTP for Li, SLi, since they have DOUBLE DeltaEV *.
28 COMPUTE L1C_half = L1C / 2.
29 COMPUTE L2C_half = L2C / 2.
30 COMPUTE L3C_half = L3C / 2.
31 COMPUTE SL1C_half = SL1C / 2.
32 COMPUTE SL2C_half = SL2C / 2.
33 COMPUTE SL3C_half = SL3C / 2.
34
35 RECODE GA_Inst (1=1) (SYSMIS=SYSMIS).
36 RECODE GB_Inst (1=2) (SYSMIS=SYSMIS).
37 RECODE GC_Inst (1=3) (SYSMIS=SYSMIS).
38
39 *trick: from this point Gj_Inst is SCALE for the Groups and the DO IFs.
40 alter type GA_Inst (f0).
41 alter type GB_Inst (f0).
42 alter type GC_Inst (f0).
43
44 DO IF (GA_Inst=1).
45     COMPUTE Groups = 1.
46     COMPUTE GroupsAB = 1.
47     COMPUTE GroupsAC = 1.
48 END IF.
49 DO IF (GB_Inst = 2).
50     COMPUTE Groups = 2.
```

A.2 Appendix: Experiment 2

```
51     COMPUTE GroupsAB = 2.
52     COMPUTE GroupsBC = 2.
53 END IF.
54 DO IF (GC.Inst = 3).
55     COMPUTE Groups = 3.
56     COMPUTE GroupsAC = 3.
57     COMPUTE GroupsBC = 3.
58 END IF.
59
60 *Compute a common 'combined' variable for all Groups lotteries, of the 3 Groups (note that corresponding
    lotteries have the same |DeltaEV| and both – or +).
61 DO IF (GA.Inst= 1).
62     COMPUTE Groups.L1A = GA.L1A.
63     COMPUTE Groups.L1B = GA.L1B.
64     COMPUTE Groups.L1C = GA.L1C.
65     COMPUTE Groups.L2A = GA.L2A.
66     COMPUTE Groups.L2B = GA.L2B.
67     COMPUTE Groups.L2C = GA.L2C.
68     COMPUTE Groups.L3A = GA.L3A.
69     COMPUTE Groups.L3B = GA.L3B.
70     COMPUTE Groups.L3C = GA.L3C.
71 END IF.
72 DO IF (GB.Inst = 2).
73     COMPUTE Groups.L1A = GB.L1A.
74     COMPUTE Groups.L1B = GB.L1B.
75     COMPUTE Groups.L1C = GB.L1C.
76     COMPUTE Groups.L2A = GB.L2A.
77     COMPUTE Groups.L2B = GB.L2B.
78     COMPUTE Groups.L2C = GB.L2C.
79     COMPUTE Groups.L3A = GB.L3A.
80     COMPUTE Groups.L3B = GB.L3B.
81     COMPUTE Groups.L3C = GB.L3C.
82 END IF.
83 DO IF (GC.Inst = 3).
84     COMPUTE Groups.L1A = GC.L1A.
85     COMPUTE Groups.L1B = GC.L1B.
86     COMPUTE Groups.L1C = GC.L1C.
87     COMPUTE Groups.L2A = GC.L2A.
88     COMPUTE Groups.L2B = GC.L2B.
89     COMPUTE Groups.L2C = GC.L2C.
90     COMPUTE Groups.L3A = GC.L3A.
91     COMPUTE Groups.L3B = GC.L3B.
92     COMPUTE Groups.L3C = GC.L3C.
93 END IF.
94
95 *Set all Delta Expected Values for Experiment plain Lotteries – All EV mean |DeltaEV| between original and
    modified lottery*.
96 COMPUTE Delta_EV.L1A = 1.25.
97 COMPUTE Delta_EV.L1B = 1.25.
98 COMPUTE Delta_EV.L1C = 2.5.
99 COMPUTE Delta_EV.L2A = 3.75.
100 COMPUTE Delta_EV.L2B = 3.75.
101 COMPUTE Delta_EV.L2C = 7.5.
102 COMPUTE Delta_EV.L3A = 12.5.
103 COMPUTE Delta_EV.L3B = 12.5.
104 COMPUTE Delta_EV.L3C = 25.
105
```

A.2 Appendix: Experiment 2

```
106 *Compute all RiskAversin (RA) variables for the One Sample t test*.
107 COMPUTE RA_L1A = L1A - Delta_EV_L1A.
108 COMPUTE RA_L1B = L1B - Delta_EV_L1B.
109 COMPUTE RA_L1C = L1C - Delta_EV_L1C.
110 COMPUTE RA_L2A = L1A - Delta_EV_L2A.
111 COMPUTE RA_L2B = L2B - Delta_EV_L2B.
112 COMPUTE RA_L2C = L2C - Delta_EV_L2C.
113 COMPUTE RA_L3A = L3A - Delta_EV_L3A.
114 COMPUTE RA_L3B = L3B - Delta_EV_L3B.
115 COMPUTE RA_L3C = L3C - Delta_EV_L3C.
116
117 *Set all Delta Expected Values for Survey Lotteries*.
118 COMPUTE Delta_EV_SL1A = 1875.
119 COMPUTE Delta_EV_SL1B = 1875.
120 COMPUTE Delta_EV_SL1C = 3750.
121 COMPUTE Delta_EV_SL2A = 5625.
122 COMPUTE Delta_EV_SL2B = 5625.
123 COMPUTE Delta_EV_SL2C = 11250.
124 COMPUTE Delta_EV_SL3A = 18750.
125 COMPUTE Delta_EV_SL3B = 18750.
126 COMPUTE Delta_EV_SL3C = 37500.
127
128 *Compute all RiskAversin (RA) variables for the One Sample t test*.
129 COMPUTE RA_SL1A = SL1A - Delta_EV_SL1A.
130 COMPUTE RA_SL1B = SL1B - Delta_EV_SL1B.
131 COMPUTE RA_SL1C = SL1C - Delta_EV_SL1C.
132 COMPUTE RA_SL2A = SL1A - Delta_EV_SL2A.
133 COMPUTE RA_SL2B = SL2B - Delta_EV_SL2B.
134 COMPUTE RA_SL2C = SL2C - Delta_EV_SL2C.
135 COMPUTE RA_SL3A = SL3A - Delta_EV_SL3A.
136 COMPUTE RA_SL3B = SL3B - Delta_EV_SL3B.
137 COMPUTE RA_SL3C = SL3C - Delta_EV_SL3C.
138
139 *Set all Expected Values for Groups*.
140 COMPUTE Delta_EV_Groups_L1A = 0.25.
141 COMPUTE Delta_EV_Groups_L1B = 0.25.
142 COMPUTE Delta_EV_Groups_L1C = 0.5.
143 COMPUTE Delta_EV_Groups_L2A = 0.75.
144 COMPUTE Delta_EV_Groups_L2B = 0.75.
145 COMPUTE Delta_EV_Groups_L2C = 1.5.
146 COMPUTE Delta_EV_Groups_L3A = 2.5.
147 COMPUTE Delta_EV_Groups_L3B = 2.5.
148 COMPUTE Delta_EV_Groups_L3C = 5.
149
150 *Compute all RiskAversin (RA) variables for the One Sample t test*.
151 COMPUTE RA_Groups_L1A = Groups_L1A - Delta_EV_Groups_L1A.
152 COMPUTE RA_Groups_L1B = Groups_L1B - Delta_EV_Groups_L1B.
153 COMPUTE RA_Groups_L1C = Groups_L1C - Delta_EV_Groups_L1C.
154 COMPUTE RA_Groups_L2A = Groups_L1A - Delta_EV_Groups_L2A.
155 COMPUTE RA_Groups_L2B = Groups_L2B - Delta_EV_Groups_L2B.
156 COMPUTE RA_Groups_L2C = Groups_L2C - Delta_EV_Groups_L2C.
157 COMPUTE RA_Groups_L3A = Groups_L3A - Delta_EV_Groups_L3A.
158 COMPUTE RA_Groups_L3B = Groups_L3B - Delta_EV_Groups_L3B.
159 COMPUTE RA_Groups_L3C = Groups_L3C - Delta_EV_Groups_L3C.
160
161 *trick: from this point Gj_Inst is NOMINAL - because Group = NOMINAL.
162 VARIABLE LEVEL GA_Inst GB_Inst GC_Inst (NOMINAL).
```

A.2 Appendix: Experiment 2

```
163
164 ***** FILTER *****
165 COMPUTE ValidCase = InfoSec.
166 alter type ValidCase (f0).
167 VARIABLE LEVEL ValidCase (SCALE).
168 *** Do not consider the CASES that took the experiment more than once – Need to add them manually ***.
169 * 192.193.116._ = many times *.
170 * 213.115.30.162 = #33, 6 min *.
171 * 188.221.164.159 = #53, 4 min *.
172 * 134.219.227.24 = twice *.
173 DO IF (V6 = '192.193.116.137' OR V6 = '192.193.116.142' OR V6 = '192.193.116.143' OR V6 = '
213.115.30.162' OR V6 = '188.221.164.159' OR V6 = '134.219.227.24').
174 COMPUTE ValidCase = 0.
175 END IF.
176
177 FILTER BY ValidCase.
178 EXECUTE.
179
180 ***** ANALYSIS *****
181
182 ***** Between Subjects *****
183 *****
184 *** HYPOTHESIS 3: Differences amongst framing–groups ***.
185
186 ** TEST: non–parametric Kruskal–Wallis: Quant (WTP) with many–categories Qual variable (Group):
187 created variable Group = 1, 2 or 3 for Groups A, B or C *.
188 ** PURPOSE of test: to show that the 3–samples WERE NOT drawn from identical populations; i.e. there
189 was DIFFERENCE amongst the 3 Treatment Groups A, B, C *.
190 * Test is on the combined variables Groups_Li{A,B,C} across the Groups = 1, 2 or 3; *.
191 * Namely, Lottery 1 Question A=Modify Probability across the 3 Groups; Question B=modify outcome;
192 Question C=avoid *.
193 ** SPSS (Kruskal–Wallis): Analyse > NonParametric Tests> Independent samples> Custom – K–W **.
194
195 ** Testing ORDER EFFECT that could be observed in the SAME variables presented to all – i.e. whether
196 the Grouping affected subjects in common variables *.
197 ** PURPOSE of test: to show that 'the 3 treatment Groups A, B, C DID NOT influence the rest
198 common–to–all–participants replies ' *.
199
200 NPTESTS
201 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B
202 RA_L3C RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B
203 RA_SL3C) GROUP (Groups) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
204 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
205 /CRITERIA ALPHA=0.05 CILEVEL=95.
206
207 * GROUP LOTTERIES BY Groups = 1 (A), 2 (B), 3 (C) *.
208 ** FINDING: WTP for Gains–framing (GroupB) much higher than WTP to avoid losses (Groups A and C) *.
209 * => If they see sure gain they invest more OR they fear NOT receiving the gain *.
210
211 NPTESTS
212 /INDEPENDENT TEST (RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A RA_Groups_L2B
213 RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C) GROUP (Groups)
214 KRUSKAL_WALLIS(COMPARE=PAIRWISE)
215 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
216 /CRITERIA ALPHA=0.05 CILEVEL=95.
217
218 ** Differences of Groups A (losses–framing) VS GroupB (gains–framing) **.
219 NPTESTS
220 /INDEPENDENT TEST (RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A
```


A.2 Appendix: Experiment 2

```
RA_Groups_L2B RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C) GROUP (
  GroupsAB) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
210 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
211 /CRITERIA ALPHA=0.05 CILEVEL=95.
212 ** Differences of Groups A (losses–framing) VS GroupC (mixed–framing) **.
213 NPTESTS
214 /INDEPENDENT TEST (RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A
  RA_Groups_L2B RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C) GROUP (
  GroupsAC) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
215 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
216 /CRITERIA ALPHA=0.05 CILEVEL=95.
217 ** Differences of Groups B (gains–framing) VS GroupC (mixed–framing) **.
218 NPTESTS
219 /INDEPENDENT TEST (RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A
  RA_Groups_L2B RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C) GROUP (
  GroupsBC) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
220 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
221 /CRITERIA ALPHA=0.05 CILEVEL=95.
222
223 ** The same tests by MAnn–Whitney, just to reveal teh distribution of the pairs of Groups **.
224 NPTESTS
225 /INDEPENDENT TEST (RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A
  RA_Groups_L2B RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C)
  GROUP (GroupsAB) MANN_WHITNEY
226 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
227 /CRITERIA ALPHA=0.05 CILEVEL=95.
228 NPTESTS
229 /INDEPENDENT TEST (RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A
  RA_Groups_L2B RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C)
  GROUP (GroupsAC) MANN_WHITNEY
230 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
231 /CRITERIA ALPHA=0.05 CILEVEL=95.
232 NPTESTS
233 /INDEPENDENT TEST (RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A
  RA_Groups_L2B RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C)
  GROUP (GroupsBC) MANN_WHITNEY
234 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
235 /CRITERIA ALPHA=0.05 CILEVEL=95.
236
237 ** Differences of Groups A (losses–framing) VS Group B (gains–framing) only for
  Subquestion C (avoidance)**.
238 NPTESTS
239 /INDEPENDENT TEST (RA_Groups_L1C RA_Groups_L2C RA_Groups_L3C) GROUP (
  GroupsAB) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
240 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
241 /CRITERIA ALPHA=0.05 CILEVEL=95.
242 ** Differences of Groups A (losses–framing) VS GroupC (mixed–framing) **.
243 NPTESTS
244 /INDEPENDENT TEST (RA_Groups_L1C RA_Groups_L2C RA_Groups_L3C) GROUP (
  GroupsAC) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
245 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
246 /CRITERIA ALPHA=0.05 CILEVEL=95.
247 ** Differences of Groups B (gains–framing) VS GroupC (mixed–framing) **.
248 NPTESTS
249 /INDEPENDENT TEST (RA_Groups_L1C RA_Groups_L2C RA_Groups_L3C) GROUP (
  GroupsBC) KRUSKAL_WALLIS(COMPARE=PAIRWISE)
250 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
```

A.2 Appendix: Experiment 2

```
251 /CRITERIA ALPHA=0.05 CILEVEL=95.
252
253 **** HYPOTHESIS 4: Four-fold pattern of Risk Attitude ****.
254
255 ** TEST: parametric One sample t test *.
256 * PURPOSE of test: whether the sample (all participants) belong to a population of a specific mean; and
    whether above (Risk Averse for losses) OR BELOW mean (Risk Seeking for losses).
257
258 * Test is on the combined variables Groups_Li{A,B,C} across the Groups = 1, 2 or 3; *.
259 * Namely, Lottery 1 Question A=Modify Probability across the 3 Groups; Question B=modify outcome;
    Question C=avoid *.
260 ** SPSS (Kruskal-Wallis): Analyse > NonParametric Tests> Independent samples> Custom – K-W **.
261
262 * EXPERIMENT LOTTERIES *.
263 ** FINDING: there is sig. diff. from mean in almost all lotteries, i.e. all subquestions B, C of L3.. *.
264 * Note: I can use mean & standard deviation of lotteries, with mu0=0 to Calculate the minimum needed
    Sample Size *.
265 T-TEST
266 /TESTVAL=0
267 /MISSING=ANALYSIS
268 /VARIABLES=RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
269 /CRITERIA=CI(.95).
270
271 T-TEST
272 /TESTVAL=0
273 /MISSING=ANALYSIS
274 /VARIABLES=L1A L1B L1C L2A L2B L2C L3A L3B L3C
275 /CRITERIA=CI(.95).
276
277 GRAPH
278 /BAR(SIMPLE)=MEAN(RA_L1A) MEAN(RA_L1B) MEAN(RA_L1C) MEAN(RA_L2A) MEAN(
    RA_L2B) MEAN(RA_L2C) MEAN(RA_L3A) MEAN(RA_L3B) MEAN(RA_L3C)
279 /MISSING=LISTWISE
280 /INTERVAL CI(95.0).
281
282 * SURVEY LOTTERIES *.
283 ** FINDING: there is sig. diff. from mean in almost all lotteries – all >mean except subquestions B, C of L3
    .. *.
284 T-TEST
285 /TESTVAL=0
286 /MISSING=ANALYSIS
287 /VARIABLES=RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C
288 /CRITERIA=CI(.95).
289
290 T-TEST
291 /TESTVAL=0
292 /MISSING=ANALYSIS
293 /VARIABLES=SL1A SL1B SL1C SL2A SL2B SL2C SL3A SL3B SL3C
294 /CRITERIA=CI(.95).
295
296 GRAPH
297 /BAR(SIMPLE)=MEAN(RA_SL1A) MEAN(RA_SL1B) MEAN(RA_SL1C) MEAN(RA_SL2A) MEAN
    (RA_SL2B) MEAN(RA_SL2C) MEAN(RA_SL3A) MEAN(RA_SL3B) MEAN(RA_SL3C)
298 /MISSING=LISTWISE
299 /INTERVAL CI(95.0).
300
301 ** One sample t test for Groups = 3 Groups**.
```

A.2 Appendix: Experiment 2

```

302      T-TEST
303          /TESTVAL=0
304          /MISSING=ANALYSIS
305          /VARIABLES=RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A
              RA_Groups_L2B RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C
306          /CRITERIA=CI(.95).
307      T-TEST
308          /TESTVAL=0
309          /MISSING=ANALYSIS
310          /VARIABLES=Groups_L1A Groups_L1B Groups_L1C Groups_L2A
              Groups_L2B Groups_L2C Groups_L3A Groups_L3B Groups_L3C
311          /CRITERIA=CI(.95).
312
313      ***** Within Subjects *****
314      *****
315      **** HYPOTHESIS 1: differences in WTP amongst risk treatment actions ****.
316      ** PURPOSE of test: examine mean differences between risk treatment actions. Actions are A&B (risk
              modification) versus C (risk transfer) *.
317
318      ** TESTS: Nonparametric Tests: Related Samples, many conditions: 1) FRIEDMAN, 2) additional FRIEDMAN
              and 3) WILCOXON PAIRWISE **.
319      ** SPSS (FRIEDMAN): Analyse > NonParametric Tests> Related samples: Fields= L2A, L2B, L3C &
              Settings= Freidman's 2-way ANOVA by ranks] **.
320      ** SPSS (additional FRIEDMAN): Analyse > NonParametric Tests> Legacy Dialogs > K-Related samples:
              set all variables, check Friedman**.
321      *then if there are differences spot them with WILCOXON pairwise tests – Here, Dependent Variable=
              WTP, Independent Variable=groups A, B, C *.
322      ** SPSS (WILCOXON): Analyse > NonParametric Tests> Legacy Dialogs > 2-Related samples: set all the
              pairs **.
323
324      *Note: the 3 Groups are not intended to measure preferences amongst Risk Treatment actions.
325      *This is why the order of subquestions A (probs), B (outcomes), C (avoidance) is the same! *
326      *therefore, we do not need to examine Risk Treatment actions WITHIN subjects from Groups A, B, C*..
327
328      * EXPERIMENT LOTTERIES *.
329      ** FINDING:
330      *Lottery1* exported files: Friedman_L1A-L1B-L1C_half-RANKS.pdf Friedman_L1A-L1B-L1C_half-
              TRIANGLE.pdf .
331      NPTESTS
332          /RELATED TEST(L1A L1B L1C_half)
333          /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
334          /CRITERIA ALPHA=0.05 CILEVEL=95.
335      *FRIEDMAN is intended to show whether there are differences initially.
336      NPAR TESTS
337          /FRIEDMAN=L1A L1B L1C_half
338          /STATISTICS DESCRIPTIVES
339          /MISSING LISTWISE.
340          *or QUANTILES*.
341      NPAR TESTS
342          /WILCOXON=L1A L1B L1C_half WITH L1B L1C_half L1A (PAIRED)
343          /MISSING ANALYSIS.
344
345      *Lottery2* exported files: Friedman_L2A-L2B-L2C_half-RANKS.pdf Friedman_L2A-L2B-L2C_half-
              TRIANGLE.pdf .
346      NPTESTS
347          /RELATED TEST(L2A L2B L2C_half ) FRIEDMAN(COMPARE=PAIRWISE)
348          /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE

```

A.2 Appendix: Experiment 2

```
349 /CRITERIA ALPHA=0.05 CILEVEL=95.
350 *additional FRIEDMAN*.
351 NPAR TESTS
352 /FRIEDMAN=L2A L2B L2C_half
353 /STATISTICS DESCRIPTIVES
354 /MISSING LISTWISE.
355 **WILCOXON pairwise**.
356 NPAR TESTS
357 /WILCOXON=L2A L2B L2C_half WITH L2B L2C_half L2A (PAIRED)
358 /MISSING ANALYSIS.
359
360 *Lottery3* exported files: Friedman_L3A–L3B–L3C_half–RANKS.pdf Friedman_L3A–L3B–L3C_half–
    TRIANGLE.pdf .
361 NPTESTS
362 /RELATED TEST(L3A L3B L3C_half ) FRIEDMAN(COMPARE=PAIRWISE)
363 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
364 /CRITERIA ALPHA=0.05 CILEVEL=95.
365 *additional FRIEDMAN*.
366 NPAR TESTS
367 /FRIEDMAN=L3A L3B L3C_half
368 /STATISTICS DESCRIPTIVES
369 /MISSING LISTWISE.
370 **WILCOXON pairwise**.
371 NPAR TESTS
372 /WILCOXON=L3A L3B L3C_half WITH L3B L3C_half L3A (PAIRED)
373 /MISSING ANALYSIS.
374
375 * SURVEY LOTTERIES *.
376 ** FINDING: for Survey Lotteries (in contrast to abstract Lotteries) there was sig diff between Probability
    and Outcome Reduction (subqs A, B) in the two realistic scenario lotteries, *.
377 * i.e. lotteries SL1 and SL2. In both lotteries WTP for reducing Outcomes > WTP for reducing
    Probabilities. This implies a REACTIVE approach to security, e.g. Disaster Recovery plans (not
    proactive) *.
378 * meaning that the recent trend [+find references] in security is observed, but also meaning that there is an
    INEVITABILITY in avoiding losses, in the first place *.
379 * It is important to mention that since, breaches are not actually invreasing [Ben WEIS2015], it might
    indeed be a paradigm shift in InfoSec *.
380 * In SL3 (p=50%) we do not have sig. diff between A and B: a possible explanation is that p=50% is easier
    to calculate rather than 5% or 15%.
381 * so maybe calculation eliminated the preference for LOSS Reduction.
382
383 *Survey Lottery1* exported files: Friedman_SL1A–SL1B–SL1C_half–RANKS.pdf Friedman_SL1A–SL1B–
    SL1C_half–TRIANGLE.pdf .
384 NPTESTS
385 /RELATED TEST(SL1A SL1B SL1C_half ) FRIEDMAN(COMPARE=PAIRWISE)
386 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
387 /CRITERIA ALPHA=0.05 CILEVEL=95.
388 *additional FRIEDMAN*.
389 NPAR TESTS
390 /FRIEDMAN=SL1A SL1B SL1C_half
391 /STATISTICS DESCRIPTIVES
392 /MISSING LISTWISE.
393 **WILCOXON pairwise**.
394 NPAR TESTS
395 /WILCOXON=SL1A SL1B SL1C_half WITH SL1B SL1C_half SL1A (PAIRED)
396 /MISSING ANALYSIS.
397
```

A.2 Appendix: Experiment 2

```
398 *Survey Lottery2* exported files: Friedman_SL2A–SL2B–SL2C_half–RANKS.pdf Friedman_SL2A–SL2B–
    SL2C_half–TRIANGLE.pdf .
399 NPTESTS
400 /RELATED TEST(SL2A SL2B SL2C_half ) FRIEDMAN(COMPARE=PAIRWISE)
401 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
402 /CRITERIA ALPHA=0.05 CILEVEL=95.
403 *additional FRIEDMAN*.
404 NPAR TESTS
405 /FRIEDMAN=SL2A SL2B SL2C_half
406 /STATISTICS DESCRIPTIVES
407 /MISSING LISTWISE.
408 **WILCOXON pairwise**.
409 NPAR TESTS
410 /WILCOXON=SL2A SL2B SL2C_half WITH SL2B SL2C_half SL2A (PAIRED)
411 /MISSING ANALYSIS.
412
413 *Survey Lottery3* exported files: Friedman_SL3A–SL3B–SL3C_half–RANKS.pdf Friedman_SL3A–SL3B–
    SL3C_half–TRIANGLE.pdf .
414 NPTESTS
415 /RELATED TEST(SL3A SL3B SL3C_half ) FRIEDMAN(COMPARE=PAIRWISE)
416 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
417 /CRITERIA ALPHA=0.05 CILEVEL=95.
418 *additional FRIEDMAN*.
419 NPAR TESTS
420 /FRIEDMAN=SL3A SL3B SL3C_half
421 /STATISTICS DESCRIPTIVES
422 /MISSING LISTWISE.
423 **WILCOXON pairwise**.
424 NPAR TESTS
425 /WILCOXON=SL3A SL3B SL3C_half WITH SL3B SL3C_half SL3A (PAIRED)
426 /MISSING ANALYSIS.
427
428 **** HYPOTHESIS 2: there is a preference between PROBABILITY and LOSSES reduction ****.
429 ** PURPOSE of test: examine mean differences between risk treatment actions A (MODIFY PROBABILITY)
    versus B (MODIFY OUTCOME) for each Lottery SLi, Li, i=1, 2, 3 *.
430 ** TEST: Nonparametric Tests: Related Samples, 2 conditions: WILCOXON PAIRWISE **.
431
432 * EXPERIMENT LOTTERIES *.
433 ** FINDING: .
434 NPAR TESTS
435 /WILCOXON=L1A WITH L1B (PAIRED)
436 /STATISTICS DESCRIPTIVES
437 /MISSING ANALYSIS.
438 NPAR TESTS
439 /WILCOXON=L2A WITH L2B (PAIRED)
440 /STATISTICS DESCRIPTIVES
441 /MISSING ANALYSIS.
442 NPAR TESTS
443 /WILCOXON=L3A WITH L3B (PAIRED)
444 /STATISTICS DESCRIPTIVES
445 /MISSING ANALYSIS.
446
447 * SURVEY LOTTERIES *.
448 ** FINDING: .
449 NPAR TESTS
450 /WILCOXON=SL1A WITH SL1B (PAIRED)
451 /STATISTICS DESCRIPTIVES
```

A.2 Appendix: Experiment 2

```
452 /MISSING ANALYSIS.
453 * FINDING sig. at SL2B > SL2A => WTP >> for MODIFY OUTCOME than MODIFY PROBABILITY, i.e.
    OUTCOMES were more 'salient' than PROBABILITIES *.more '!'.
454 NPAR TESTS
455 /WILCOXON=SL2A WITH SL2B (PAIRED)
456 /STATISTICS DESCRIPTIVES
457 /MISSING ANALYSIS.
458 NPAR TESTS
459 /WILCOXON=SL3A WITH SL3B (PAIRED)
460 /STATISTICS DESCRIPTIVES
461 /MISSING ANALYSIS.
462
463 * Note: the same test can be used as VALIDITY CHECK for Lotteries of the Groups *.
464 NPAR TESTS
465 /WILCOXON=Groups_L1A Groups_L1B Groups_L1C
466 /MISSING ANALYSIS.
467 NPAR TESTS
468 /WILCOXON=Groups_L2A Groups_L2B Groups_L2C
469 /MISSING ANALYSIS.
470 NPAR TESTS
471 /WILCOXON=Groups_L3A Groups_L3B Groups_L3C
472 /MISSING ANALYSIS.
473
474 ***** Survey Data Analysis *****.
475 **** A) Descriptive Statistics *****.
476 FREQUENCIES VARIABLES=InfoSec Risk
477 /HISTOGRAM
478 /ORDER=ANALYSIS.
479 FREQUENCIES VARIABLES=Gender
480 /HISTOGRAM
481 /ORDER=ANALYSIS.
482 GRAPH
483 /PIE=COUNT BY Edu.
484
485 FREQUENCIES VARIABLES=Cur_pos Age Exp
486 /HISTOGRAM
487 /ORDER=ANALYSIS.
488 FREQUENCIES VARIABLES=Gender
489 /HISTOGRAM
490 /ORDER=ANALYSIS.
491
492 **** B) Spearman correlations *****.
493 ** Spearman: Quant with Quant variables **.
494 * FINDING: some negative correlation between Cur_Position and WTP in L3j: i.e. the more years in the position
    the more risk taking they became .
495 NONPAR CORR
496 /VARIABLES=Risk Age Dependants Worried RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A
    RA_L3B RA_L3C RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B
    RA_SL3C
497 /PRINT=SPEARMAN TWOTAIL NOSIG
498 /MISSING=PAIRWISE.
499 * FINDING: negative correlation between Age and WTP, mostly (4 by 1) for Survey Lotteries! .
500 ** Speraman's Correlation: shows MONOTONIC relationship (both variables need to be ORDINAL,
    INTERVAL or RATIO scale) ** (more specialised than Pearson's).
501 NONPAR CORR
502 /VARIABLES=Cur_pos Age Exp RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B
    RA_L3C RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B
```

A.2 Appendix: Experiment 2

```
RA_SL3C
503 /PRINT=SPEARMAN TWOTAIL NOSIG
504 /MISSING=PAIRWISE.
505 ** Pearson's Correlation: shows LINEAR relationship (both variables need to be INTERvAL or RATIO
scale) **.
506 CORRELATIONS
507 /VARIABLES=Cur_pos Age Exp RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B
RA_L3C RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B
RA_SL3C
508 /PRINT=TWOTAIL NOSIG
509 /MISSING=PAIRWISE.
510 CORRELATIONS
511 /VARIABLES=Cur_pos Age Exp RA_SL3C
512 /PRINT=TWOTAIL NOSIG
513 /MISSING=PAIRWISE.
514
515 FREQUENCIES Cur_pos Age Exp RA_SL3C
516 /ORDER=ANALYSIS.
517
518 **** C) Mann–Whitney: Quant with binary Qual (Nominal) variables **.
519 * Gender *.
520 NPTESTS
521 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
Gender) MANN_WHITNEY
522 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
523 /CRITERIA ALPHA=0.05 CILEVEL=95.
524 * English *.
525 NPTESTS
526 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
English) MANN_WHITNEY
527 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
528 /CRITERIA ALPHA=0.05 CILEVEL=95.
529 * Protect *.
530 NPTESTS
531 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
Protect) MANN_WHITNEY
532 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
533 /CRITERIA ALPHA=0.05 CILEVEL=95.
534 * Indep *.
535 NPTESTS
536 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
Indep) MANN_WHITNEY
537 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
538 /CRITERIA ALPHA=0.05 CILEVEL=95.
539 * Incident *.
540 NPTESTS
541 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
Incident) MANN_WHITNEY
542 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
543 /CRITERIA ALPHA=0.05 CILEVEL=95.
544
545 ** D) Kruskal–Wallis: Quant with many–categories Qual variables **.
```

A.2 Appendix: Experiment 2

```
546 * Income *.
547 NPTESTS
548 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
      RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
      Income)
549 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
550 /CRITERIA ALPHA=0.05 CILEVEL=95.
551 * Employees *.
552 NPTESTS
553 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
      RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
      Employees)
554 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
555 /CRITERIA ALPHA=0.05 CILEVEL=95.
556 * Edu *.
557 NPTESTS
558 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
      RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
      Edu)
559 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
560 /CRITERIA ALPHA=0.05 CILEVEL=95.
561 * Worried *.
562 NPTESTS
563 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
      RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
      Worried)
564 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
565 /CRITERIA ALPHA=0.05 CILEVEL=95.
566 * Marital .
567 NPTESTS
568 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
      RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
      Marital)
569 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
570 /CRITERIA ALPHA=0.05 CILEVEL=95.
571 * Job *.
572 NPTESTS
573 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
      RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
      Job)
574 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
575 /CRITERIA ALPHA=0.05 CILEVEL=95.
576 * PaymentLottery *.
577 NPTESTS
578 /INDEPENDENT TEST (RA_L1A RA_L1B RA_L1C RA_L2A RA_L2B RA_L2C RA_L3A RA_L3B RA_L3C
      RA_SL1A RA_SL1B RA_SL1C RA_SL2A RA_SL2B RA_SL2C RA_SL3A RA_SL3B RA_SL3C) GROUP (
      PaymentLottery)
579 /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
580 /CRITERIA ALPHA=0.05 CILEVEL=95.
581
582 *** E) Chi-square (Pearson): Qual with Qual [the first Sig. is the one] ***.
583 * Sec VS OPS BY Past Incident*.
584 CROSSTABS
585 /TABLES=Gender BY Job
586 /FORMAT=AVALUE TABLES
587 /STATISTICS=CHISQ
588 /CELLS=COUNT
```


A.2 Appendix: Experiment 2

```
589 /COUNT ROUND CELL.
590 * Sec VS OPS BY Job Title [SIG.]*.
591 *CROSSTABS
592 /TABLES=H5_1_1_1 BY S12
593 /FORMAT=AVALUE TABLES
594 /STATISTICS=CHISQ
595 /CELLS=COUNT
596 /COUNT ROUND CELL.
597 * Sec VS OPS BY Educational Level *.
598 CROSSTABS
599 /TABLES=Edu BY Job
600 /FORMAT=AVALUE TABLES
601 /STATISTICS=CHISQ
602 /CELLS=COUNT
603 /COUNT ROUND CELL.
604 * Sec VS OPS BY Annual Salary *.
605 CROSSTABS
606 /TABLES=Marital BY Gender
607 /FORMAT=AVALUE TABLES
608 /STATISTICS=CHISQ
609 /CELLS=COUNT
610 /COUNT ROUND CELL.
611
612 **** F) Multiple Regressions.
613 **** Multiple Regression Analysis *****.
614 ** a FORWARD Regression for each Dependent Variable **.
615 ** findings: IV=Employees, with CONTROL VARS=Exp Age and DV=Li **.
616 REGRESSION
617 /MISSING LISTWISE
618 /STATISTICS COEFF OUTS R ANOVA
619 /CRITERIA=PIN(.05) POUT(.10)
620 /NOORIGIN
621 /DEPENDENT L1A
622 /METHOD=ENTER Exp Age Cur_Pos .
623 REGRESSION
624 /MISSING LISTWISE
625 /STATISTICS COEFF OUTS R ANOVA
626 /CRITERIA=PIN(.05) POUT(.10)
627 /NOORIGIN
628 /DEPENDENT L1B
629 /METHOD=ENTER Exp Age Cur_Pos .
630 REGRESSION
631 /MISSING LISTWISE
632 /STATISTICS COEFF OUTS R ANOVA
633 /CRITERIA=PIN(.05) POUT(.10)
634 /NOORIGIN
635 /DEPENDENT L1C
636 /METHOD=ENTER Exp Age Cur_Pos .
637
638 REGRESSION
639 /MISSING LISTWISE
640 /STATISTICS COEFF OUTS R ANOVA
641 /CRITERIA=PIN(.05) POUT(.10)
642 /NOORIGIN
643 /DEPENDENT L2A
644 /METHOD=ENTER Exp Age Cur_Pos .
645 REGRESSION
```

A.2 Appendix: Experiment 2

```
646 /MISSING LISTWISE
647 /STATISTICS COEFF OUTS R ANOVA
648 /CRITERIA=PIN(.05) POUT(.10)
649 /NOORIGIN
650 /DEPENDENT L2B
651 /METHOD=ENTER Exp Age Cur_Pos .
652 REGRESSION
653 /MISSING LISTWISE
654 /STATISTICS COEFF OUTS R ANOVA
655 /CRITERIA=PIN(.05) POUT(.10)
656 /NOORIGIN
657 /DEPENDENT L2C
658 /METHOD=ENTER Exp Age Cur_Pos .
659
660 REGRESSION
661 /MISSING LISTWISE
662 /STATISTICS COEFF OUTS R ANOVA
663 /CRITERIA=PIN(.05) POUT(.10)
664 /NOORIGIN
665 /DEPENDENT L3A
666 /METHOD=ENTER Exp Age Cur_Pos .
667 REGRESSION
668 /MISSING LISTWISE
669 /STATISTICS COEFF OUTS R ANOVA
670 /CRITERIA=PIN(.05) POUT(.10)
671 /NOORIGIN
672 /DEPENDENT L3B
673 /METHOD=ENTER Exp Age Cur_Pos .
674 REGRESSION
675 /MISSING LISTWISE
676 /STATISTICS COEFF OUTS R ANOVA
677 /CRITERIA=PIN(.05) POUT(.10)
678 /NOORIGIN
679 /DEPENDENT L3C
680 /METHOD=ENTER Exp Age Cur_Pos .
681
682 ***** with Survey Lotteries *****.
683 REGRESSION
684 /MISSING LISTWISE
685 /STATISTICS COEFF OUTS R ANOVA
686 /CRITERIA=PIN(.05) POUT(.10)
687 /NOORIGIN
688 /DEPENDENT SL1A
689 /METHOD=ENTER Exp Age Cur_Pos .
690 REGRESSION
691 /MISSING LISTWISE
692 /STATISTICS COEFF OUTS R ANOVA
693 /CRITERIA=PIN(.05) POUT(.10)
694 /NOORIGIN
695 /DEPENDENT SL1B
696 /METHOD=ENTER Exp Age Cur_Pos .
697 REGRESSION
698 /MISSING LISTWISE
699 /STATISTICS COEFF OUTS R ANOVA
700 /CRITERIA=PIN(.05) POUT(.10)
701 /NOORIGIN
702 /DEPENDENT SL1C
```

A.2 Appendix: Experiment 2

```
703 /METHOD=ENTER Exp Age Cur_Pos .
704
705 REGRESSION
706 /MISSING LISTWISE
707 /STATISTICS COEFF OUTS R ANOVA
708 /CRITERIA=PIN(.05) POUT(.10)
709 /NOORIGIN
710 /DEPENDENT SL2A
711 /METHOD=ENTER Exp Age Cur_Pos .
712 REGRESSION
713 /MISSING LISTWISE
714 /STATISTICS COEFF OUTS R ANOVA
715 /CRITERIA=PIN(.05) POUT(.10)
716 /NOORIGIN
717 /DEPENDENT SL2B
718 /METHOD=ENTER Exp Age Cur_Pos .
719 REGRESSION
720 /MISSING LISTWISE
721 /STATISTICS COEFF OUTS R ANOVA
722 /CRITERIA=PIN(.05) POUT(.10)
723 /NOORIGIN
724 /DEPENDENT SL2C
725 /METHOD=ENTER Exp Age Cur_Pos .
726
727 REGRESSION
728 /MISSING LISTWISE
729 /STATISTICS COEFF OUTS R ANOVA
730 /CRITERIA=PIN(.05) POUT(.10)
731 /NOORIGIN
732 /DEPENDENT SL3A
733 /METHOD=ENTER Exp Age Cur_Pos .
734 REGRESSION
735 /MISSING LISTWISE
736 /STATISTICS COEFF OUTS R ANOVA
737 /CRITERIA=PIN(.05) POUT(.10)
738 /NOORIGIN
739 /DEPENDENT SL3B
740 /METHOD=ENTER Exp Age Cur_Pos .
741 REGRESSION
742 /MISSING LISTWISE
743 /STATISTICS COEFF OUTS R ANOVA
744 /CRITERIA=PIN(.05) POUT(.10)
745 /NOORIGIN
746 /DEPENDENT SL3C
747 /METHOD=ENTER Exp Age Cur_Pos .
748
749 REGRESSION
750 /MISSING LISTWISE
751 /STATISTICS COEFF OUTS R ANOVA
752 /CRITERIA=PIN(.05) POUT(.10)
753 /NOORIGIN
754 /DEPENDENT RiskAversionH2_6
755 /METHOD=ENTER S4cat S10_1 S13 S19 S22_1.
756
757 * 'How willing are you yo sacrifice Pos for Sec?' (S11_1)*.
758 NONPAR CORR
759 /VARIABLES=S11_1 SWITCHPOINT_SEC LOSS_AV_SEC SWITCHPOINT_OPS LOSS_AV_OPS
```

A.2 Appendix: Experiment 2

```
760 /PRINT=SPEARMAN TWOTAIL NOSIG
761 /MISSING=PAIRWISE.
762 * as expected (?) *.
763 NONPAR CORR
764 /VARIABLES=SWITCHPOINT_SEC LOSS_AV_SEC SWITCHPOINT_OPS LOSS_AV_OPS
765 /PRINT=SPEARMAN TWOTAIL NOSIG
766 /MISSING=PAIRWISE.
767 *non-parametric.
768 NONPAR CORR
769 /VARIABLES= L3C Risk
770 /PRINT=SPEARMAN TWOTAIL NOSIG
771 /MISSING=PAIRWISE.
772
773 ***** Various Validity checks *****.
774 desc var = Groups.
775 desc var = GA_Inst GB_Inst GC_Inst.
776
777 FREQUENCIES InfoSec Groups Q117
778 /ORDER=ANALYSIS.
779 EXAMINE VARIABLES= L1A L1B L1C L2A L2B L2C L3A L3B L3C BY English
780 /COMPARE VARIABLE
781 /PLOT=BOXPLOT
782 /STATISTICS=NONE
783 /NOTOTAL
784 /MISSING=PAIRWISE.
785 EXAMINE VARIABLES= SL1A SL1B SL1C SL2A SL2B SL2C SL3A SL3B SL3C BY English
786 /COMPARE VARIABLE
787 /PLOT=BOXPLOT
788 /STATISTICS=NONE
789 /NOTOTAL
790 /MISSING=PAIRWISE.
791 EXAMINE VARIABLES= RA_Groups_L1A RA_Groups_L1B RA_Groups_L1C RA_Groups_L2A RA_Groups_L2B
RA_Groups_L2C RA_Groups_L3A RA_Groups_L3B RA_Groups_L3C BY English
792 /COMPARE VARIABLE
793 /PLOT=BOXPLOT
794 /STATISTICS=NONE
795 /NOTOTAL
796 /MISSING=PAIRWISE.
797
798 * Tests for Normality: Kolmogorov-Smirnov & Sharpio-Wilk *.
799 EXAMINE VARIABLES=SL1A SL1B SL1C
800 /PLOT BOXPLOT NPLOT
801 /COMPARE GROUPS
802 /STATISTICS DESCRIPTIVES
803 /CINTERVAL 95
804 /MISSING LISTWISE
805 /NOTOTAL.
806
807 * I do a Descriptive Statistics > Explore analysis with Steam&Leaf plot and Boxplots.
808 * There are initial conclusions on the Skewness (left or right) and the Kurtosis (leptokurtosis or platycurtosis) of
the distribution.
809 EXAMINE VARIABLES=L1A L1B L1C L2A L2B L2C L3A L3B L3C
810 /PLOT BOXPLOT STEMLEAF
811 /COMPARE GROUPS
812 /STATISTICS DESCRIPTIVES
813 /CINTERVAL 95
814 /MISSING LISTWISE
```

A.2 Appendix: Experiment 2

```

815 /NOTOTAL.
816 *Boxplot of all Questions of H1 in the same Graphic (option: Data are Separate Variables). .
817 EXAMINE VARIABLES=L1A L1B L1C L2A L2B L2C L3A L3B L3C
818 /COMPARE VARIABLE
819 /PLOT=BOXPLOT
820 /STATISTICS=NONE
821 /NOTOTAL
822 /MISSING=PAIRWISE.
823 *Boxplot of all Questions of H1 in the same Graphic (option: Data are Separate Variables). .
824 EXAMINE VARIABLES=SL1A SL1B SL1C SL2A SL2B SL2C SL3A SL3B SL3C
825 /COMPARE VARIABLE
826 /PLOT=BOXPLOT
827 /STATISTICS=NONE
828 /NOTOTAL
829 /MISSING=PAIRWISE.
830
831 ***** Normality test for parametric one--sample t--test -- for APPENDIX *****.
832 *Computes the z--values for the specified values AND SAVES them in new variables (starting with zVAR) --.
833 DESCRIPTIVES VARIABLES=L1A L1B L1C L2A L2B L2C L3A L3B L3C SL1A SL1B SL1C SL2A SL2B SL2C
      SL3A SL3B SL3C
834 /SAVE
835 /STATISTICS=MEAN STDDEV MIN MAX.
836 *Descriptives for all variables of all lotteries*.
837 *EXAMINE VARIABLES=L1A L1B L1C L2A L2B L2C L3A L3B L3C SL1A SL1B SL1C SL2A SL2B SL2C
      SL3A SL3B SL3C
838 /PLOT BOXPLOT STEMLEAF
839 /COMPARE GROUPS
840 /MESTIMATORS HUBER(1.339) ANDREW(1.34) HAMPEL(1.7,3.4,8.5) TUKEY(4.685)
841 /PERCENTILES(5,10,25,50,75,90,95) HAVERAGE
842 /STATISTICS DESCRIPTIVES EXTREME
843 /CINTERVAL 95
844 /MISSING LISTWISE
845 /NOTOTAL.
846 *Boxplot of all Questions of H1 in the same Graphic (option: Data are Separate Variables).
847 *Also used to define the limits for variable DUMMY.
848 EXAMINE VARIABLES=L1A L1B L1C L2A L2B L2C L3A L3B L3C SL1A SL1B SL1C SL2A SL2B SL2C
      SL3A SL3B SL3C
849 /COMPARE VARIABLE
850 /PLOT=BOXPLOT
851 /STATISTICS=NONE
852 /NOTOTAL
853 /MISSING=PAIRWISE.
854
855 **** Detecting OUTLIERS from z--scores: if cum. % of Std. Deviation > 1.96 is about 5%, then we are fine! *
      ***.
856 * L1A *.
857 DESCRIPTIVES
858 VARIABLES=L1A/SAVE.
859 COMPUTE zL1A=abs(zL1A).
860 RECODE zL1A (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
861 VALUE LABELS zL1A
862 4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
863 FREQUENCIES
864 VARIABLES=zL1A
865 /ORDER=ANALYSIS.
866 * L1B *.

```

A.2 Appendix: Experiment 2

```
867 DESCRIPTIVES
868 VARIABLES=L1B/SAVE.
869 COMPUTE zL1B=abs(zL1B).
870 RECODE zL1B (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
871 VALUE LABELS zL1B
872     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
873 FREQUENCIES
874     VARIABLES=zL1B
875     /ORDER=ANALYSIS.
876     * L1C *.
877 DESCRIPTIVES
878 VARIABLES=L1C/SAVE.
879 COMPUTE zL1C=abs(zL1C).
880 RECODE zL1C (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
881 VALUE LABELS zL1C
882     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
883 FREQUENCIES
884     VARIABLES=zL1C
885     /ORDER=ANALYSIS.
886     * L2A *.
887 DESCRIPTIVES
888 VARIABLES=L2A/SAVE.
889 COMPUTE zL2A=abs(zL2A).
890 RECODE zL2A (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
891 VALUE LABELS zL2A
892     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
893 FREQUENCIES
894     VARIABLES=zL2A
895     /ORDER=ANALYSIS.
896     * L2B *.
897 DESCRIPTIVES
898 VARIABLES=L2B/SAVE.
899 COMPUTE zL2B=abs(zL2B).
900 RECODE zL2B (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
901 VALUE LABELS zL2B
902     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
903 FREQUENCIES
904     VARIABLES=zL2B
905     /ORDER=ANALYSIS.
906     * L2C *.
907 DESCRIPTIVES
908 VARIABLES=L2C/SAVE.
909 COMPUTE zL2C=abs(zL2C).
910 RECODE zL2C (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
911 VALUE LABELS zL2C
912     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
913 FREQUENCIES
914     VARIABLES=zL2C
915     /ORDER=ANALYSIS.
916     * L3A *.
917 DESCRIPTIVES
918 VARIABLES=L3A/SAVE.
```

A.2 Appendix: Experiment 2

```
919 COMPUTE zL3A=abs(zL3A).
920 RECODE zL3A (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
921 VALUE LABELS zL3A
922     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
923 FREQUENCIES
924     VARIABLES=zL3A
925 /ORDER=ANALYSIS.
926 * L3B *.
927 DESCRIPTIVES
928 VARIABLES=L3B/SAVE.
929 COMPUTE zL3B=abs(zL3B).
930 RECODE zL3B (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
931 VALUE LABELS zL3B
932     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
933 FREQUENCIES
934     VARIABLES=zL3B
935 /ORDER=ANALYSIS.
936 * L3C *.
937 DESCRIPTIVES
938 VARIABLES=L3C/SAVE.
939 COMPUTE zL3C=abs(zL3C).
940 RECODE zL3C (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4).
941 VALUE LABELS zL3C
942     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
943 FREQUENCIES
944     VARIABLES=zL3C
945 /ORDER=ANALYSIS.
946 ** The same for Survey lotteries **.
947 * SL1A *.
948 DESCRIPTIVES
949 VARIABLES=SL1A/SAVE.
950 COMPUTE zSL1A=abs(zSL1A).
951 RECODE zSL1A (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
      .
952 VALUE LABELS zSL1A
953     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
954 FREQUENCIES
955     VARIABLES=zSL1A
956 /ORDER=ANALYSIS.
957 * SL1B *.
958 DESCRIPTIVES
959 VARIABLES=SL1B/SAVE.
960 COMPUTE zSL1B=abs(zSL1B).
961 RECODE zSL1B (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
      .
962 VALUE LABELS zSL1B
963     4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
964 FREQUENCIES
965     VARIABLES=zSL1B
966 /ORDER=ANALYSIS.
967 * SL1C *.
968 DESCRIPTIVES
```

A.2 Appendix: Experiment 2

```
969  VARIABLES=SL1C/SAVE.
970  COMPUTE zSL1C=abs(zSL1C).
971  RECODE zSL1C (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
972  VALUE LABELS zSL1C
973    4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
974  FREQUENCIES
975    VARIABLES=zSL1C
976    /ORDER=ANALYSIS.
977    * SL2A *.
978  DESCRIPTIVES
979  VARIABLES=SL2A/SAVE.
980  COMPUTE zSL2A=abs(zSL2A).
981  RECODE zSL2A (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
982  VALUE LABELS zSL2A
983    4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
984  FREQUENCIES
985    VARIABLES=zSL2A
986    /ORDER=ANALYSIS.
987    * SL2B *.
988  DESCRIPTIVES
989  VARIABLES=SL2B/SAVE.
990  COMPUTE zSL2B=abs(zSL2B).
991  RECODE zSL2B (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
992  VALUE LABELS zSL2B
993    4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
994  FREQUENCIES
995    VARIABLES=zSL2B
996    /ORDER=ANALYSIS.
997    * SL2C *.
998  DESCRIPTIVES
999  VARIABLES=SL2C/SAVE.
1000 COMPUTE zSL2C=abs(zSL2C).
1001 RECODE zSL2C (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
1002 VALUE LABELS zSL2C
1003    4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
1004 FREQUENCIES
1005    VARIABLES=zSL2C
1006    /ORDER=ANALYSIS.
1007    * SL3A *.
1008 DESCRIPTIVES
1009 VARIABLES=SL3A/SAVE.
1010 COMPUTE zSL3A=abs(zSL3A).
1011 RECODE zSL3A (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
1012 VALUE LABELS zSL3A
1013    4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
      Outliers (z>3.29)'.
1014 FREQUENCIES
1015    VARIABLES=zSL3A
```


A.2 Appendix: Experiment 2

```
1016 /ORDER=ANALYSIS.
1017 * SL3B *.
1018 DESCRIPTIVES
1019 VARIABLES=SL3B/SAVE.
1020 COMPUTE zSL3B=abs(zSL3B).
1021 RECODE zSL3B (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
1022 VALUE LABELS zSL3B
1023 4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
Outliers (z>3.29)'.
1024 FREQUENCIES
1025 VARIABLES=zSL3B
1026 /ORDER=ANALYSIS.
1027 * SL3C *.
1028 DESCRIPTIVES
1029 VARIABLES=SL3C/SAVE.
1030 COMPUTE zSL3C=abs(zSL3C).
1031 RECODE zSL3C (3.29 thru highest = 1)(2.58 thru highest = 2)(1.96 thru highest = 3)(Lowest thru 1.95 = 4)
.
1032 VALUE LABELS zSL3C
1033 4 'Normal range' 3 'Potential Outliers (1.96<z<2.58)' 2 'Probabe Outliers (2.58<z<3.29)' 1 'Extreme
Outliers (z>3.29)'.
1034 FREQUENCIES
1035 VARIABLES=zSL3C
1036 /ORDER=ANALYSIS.
1037
1038 DESCRIPTIVES VARIABLES=L1A L1B L1C_half L2A L2B L2C_half L3A L3B L3C_half
1039 /STATISTICS=MEAN STDDEV RANGE MIN MAX SEMEAN.
1040
1041 DESCRIPTIVES VARIABLES=SL1A SL1B SL1C_half SL2A SL2B SL2C_half SL3A SL3B SL3C_half
1042 /STATISTICS=MEAN STDDEV RANGE MIN MAX SEMEAN.
1043
1044 DESCRIPTIVES VARIABLES=L1A L1B L1C L2A L2B L2C L3A L3B L3C RA_L1A RA_L1B RA_L1C RA_L2A
RA_L2B
1045 RA_L2C RA_L3A RA_L3B RA_L3C
1046 /STATISTICS=MEAN STDDEV RANGE MIN MAX SEMEAN.
```

A.3 Appendix: Modelling Investment Decisions

A.3.0.1 Marginal Preferences and Traces on levels

Marginal preferences are a sort of projection of the global preference \succeq on each attribute i and, more precisely, on each subset I of attributes, so that vectors of space A can be compared by “fixing” a number of their coordinates a_i and allowing the rest of the attributes w_{-i} that do not belong to subset I to vary. Marginal traces also allow for such comparisons, but they provide more information regarding the alternatives containing the w_{-i} [33].

Marginal preferences are defined as: $a_i \succeq b_i \Leftrightarrow (i, w_{-i})(i, w_{-i}), \forall w_{-i} \in A_{-I}$, where a_i are vectors on subspace A_I and w_{-i} on A_{-I} .

Marginal traces on levels are defined as: $\forall a_i, b_i \in A_I, \forall w_{-i} \in A_{-I}, \forall k \in A$:

1. $a_i \succeq^+ b_i \Leftrightarrow [(b_i, w_{-i}) \geq k \Rightarrow (a_i, w_{-i}) \geq k]$
2. $a_i \succeq^- b_i \Leftrightarrow [k \succeq (a_i, w_{-i}) \Rightarrow k(b_i, w_{-i})]$
3. $a_i \succeq^\pm b_i \Leftrightarrow \begin{cases} (b_i, w_{-i}) \geq k \Rightarrow (a_i, w_{-i}) \geq k \\ \text{and} \\ k \succeq (a_i, w_{-i}) \Rightarrow k(b_i, w_{-i}) \end{cases}$

If we consider the attributes: security, operational time and monetary amount, then the set of all attributes is $\{1, 2, 3\} \equiv \{SEC, OPS, Z\}$ and, e.g. for subset $I = \{1, 3\}$ we have:

$a_i \succeq b_i$ i.e. $(s_1, z_1) \succeq (s_2, z_2) \Rightarrow (s_1, o_1, z_1) \succeq (s_2, o_2, z_2), \forall o_1, o_2 \in A_2 = A_{-I}$.

$a_i \succeq^+ b_i$ i.e. $(s_2, o_1, z_2) \succeq k \Rightarrow (s_1, o_2, z_1) \succeq k, \forall o_1, o_2 \in A_2 = A_{-I}$.

$a_i \succeq^- b_i$ i.e. $k \succeq (s_1, o_1, z_1) \Rightarrow k \succeq (s_2, o_2, z_2), \forall o_1, o_2 \in A_2 = A_{-I}$.

For the particular context of information security investment, it is intuitively apparent that not all “subsets I” of attributes allow for marginal preferences and marginal traces to be defined on the attribute levels α_i and β_i . The question which arises then, is whether the allowed “subsets I” can be empirically elicited through experiments. The necessary conditions which will allow for the constructive proof of existence of a (unique) preference relation can be empirically tested [95].

Conjoint Analysis is a statistical methodology that emanated from conjoint measurement theory that allows for the empirical elicitation of stated preferences.

A.4 Appendix: Supplementary Survey

A.4.0.1 Supplementary Survey

Question 1: “Are you related with the profession or practice of Information Security in any way?”

Question 2: Question: “Your current or last job role most closely resembles:”

- Senior executive role
(e.g. CEO, CIO, CISO, CSO etc.)
- Managerial role
(e.g. Project Manager, IT Director, Security Manager etc.)
- IT & Security
(e.g. Security Officer, System Admin, Cyber Security Information Analyst etc.)
- Compliance, Risk or Privacy role
(e.g. Governance, Risk and Compliance Consultant, Information Security Consultant, Auditor etc.)
- Other: please specify

Questions related to Perception of Risk & Skills:

Question 3: “In your opinion, how willing are Information Security Professionals to take risks?”
(not willing at all, mostly not willing, neither willing nor not-willing, somewhat willing, very willing)

Question 4: “Do you think that your mathematical abilities are better than the average person’s?” (e.g. with respect to probabilities and expected values)
(not better at all, mostly not better, the same, somewhat better, much better)

Question 5: “How willing are you to take risks in general?”
(not willing at all, mostly not willing, neither willing nor not-willing, somewhat willing, very willing)

A.4 Appendix: Supplementary Survey

Question 6: “Which one of the following gambles do you instinctively prefer, by first look?”

You have to roll a dice,

(Gamble A) If a ‘5’ or a ‘6’ comes up, you win (or better use ‘lose’?) \$10

(Gamble B) If a ‘6’ comes up, you win (or better use ‘lose’?) \$20

Question 7: “Imagine you are responsible for the Information Security budget and you have to consider potential information security threats. Evaluate and rank the following statements from the most important to the least important:”

- Estimating expected losses, e.g. $\text{Asset Value} \times \text{Vulnerability} \times \text{Threat Probability}$
- Considering losses of the worst-case scenario
- Estimating a specific probability of loss instead of a range of probabilities
- Prioritising security of the system
- Prioritising operational time of tasks
- Investing in security measures for small-probability threats
- Investing in security measures for large-probability threats
- Eliminating existing risk completely
- Containing potential monetary losses in case of a security incident
- Reducing the vulnerabilities of the system
- Obtaining appropriate insurance

A.4 Appendix: Supplementary Survey

Question 8: “Imagine you are responsible for Information Security budget and you have to consider potential information security threats. Which of the following items do you consider important?”

- Estimating expected losses, e.g. Asset Value × Vulnerability × Threat Probability
- Considering losses of the worst-case scenario
- Estimating a specific probability of loss instead of a range of probabilities
- Prioritising security of the system
- Prioritising operational time of tasks
- Investing in security measures for small-probability threats
- Investing in security measures for large-probability threats
- Eliminating existing risk completely
- Containing potential monetary losses in case of a security incident
- Reducing the vulnerabilities of the system
- Obtaining appropriate insurance

Questions related to Professional Role:

Question 9: “Are you less or more risk seeking in your []^a role than in your personal life?”

(much less risk seeking in my professional role, somewhat less risk seeking, the same, somewhat more risk seeking, much more risk seeking in my professional role)

^aParticipants were presented with their role, as stated in Question 2.

Question 10: “Are you less or more risk seeking than your colleagues in your []^a role?”

(less risk seeking than colleagues, somewhat less risk seeking, the same, somewhat more risk seeking, more risk seeking than colleagues)

^aParticipants were presented with their role, as stated in Question 2.

A.4 Appendix: Supplementary Survey

Question 11: “In your opinion, the perceived importance of which of the following statements does your []^a role affect, making you more careful or worried?”

- Estimating expected losses, e.g. Asset Value × Vulnerability × Threat Probability
- Considering losses of the worst-case scenario
- Estimating a specific probability of loss instead of a range of probabilities
- Prioritising security of the system
- Prioritising operational time of tasks
- Investing in security measures for small-probability threats
- Investing in security measures for large-probability threats
- Eliminating existing risk completely
- Containing potential losses in case of a security incident
- Reducing the vulnerabilities of the system
- Obtaining appropriate insurance

^aParticipants were presented with their role, as stated in Question 2.

Question 12: “In your opinion, the perceived importance of which of the two attributes: Security or Operational Time, is affected by the following professional roles?”

	Attribute that is perceived as more important:	
	Security	Operational Time
Senior executive role (e.g. CEO, CIO, CISO, CSO etc.)	<input type="checkbox"/>	<input type="checkbox"/>
Managerial role (e.g. Project Manager, IT Director, Security Manager etc.)	<input type="checkbox"/>	<input type="checkbox"/>
IT & Security (e.g. Security Officer, System Admin, Cyber Security Information Analyst etc.)	<input type="checkbox"/>	<input type="checkbox"/>
Compliance, Risk or Privacy role (e.g. Governance, Risk and Compliance Consultant, Information Security Consultant, Auditor etc.)	<input type="checkbox"/>	<input type="checkbox"/>

A.4 Appendix: Supplementary Survey

Question 13: “How willing are you to take risks in your []^a role?”
(not willing at all, mostly not willing, neither willing nor not-willing, somewhat willing, very willing)

^aParticipants were presented with their role, as stated in Question 2.

Bibliography

- [1] IBM SPSS statistics for Windows, Version 21.0. Armonk, NY:IBM Corp., IBM Corp. Released 2012.
- [2] Wolfram Research, Inc., Mathematica, Version 9.0, Champaign, Illinois, USA, 2012.
- [3] Qualtrics software, Version 37. Qualtrics Provo, Utah, USA, 2013.
- [4] Cost of business cyber security breaches almost double. Technical report, Department for Business, Innovation and Skills (BIS, UK) and Technology Strategy Board, April 2014. <https://www.gov.uk/government/news/cost-of-business-cyber-security-breaches-almost-double>. Last accessed on 09/09/2016.
- [5] A. Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*, pages 21–29. ACM, 2004.
- [6] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 2:24–30, 2005.
- [7] A. Acquisti and J. Grossklags. What can behavioral economics teach us about privacy. *Digital privacy*, page 329, 2007.
- [8] D. Alexander, A. Finch, and D. Sutton. Information Security Management Principles. BCS, 2013.
- [9] M. Allais. Le comportement de l’homme rationnel devant le risque: critique des postulats et axiomes de l’école américaine. *Econometrica: Journal of the Econometric Society*, pages 503–546, 1953.
- [10] S. Anagol, S. Bennett, G. Bryan, T. Davenport, N. Hite, D. Karlan, P. Lagunes, and M. McConnell. There’s something about ambiguity. Working Paper, Yale, 2008.

- [11] R. Anderson. Why Information Security is Hard - An Economic Perspective. In *Proceedings of 17th Annual Computer Security Applications Conference (AC-SAC)*. New Orleans, Louisiana, Dec. 10–14, 2001.
- [12] R. Anderson. Information Security Economics-and Beyond. In *Deontic Logic in Computer Science*, pages 49–49. Springer, 2008.
- [13] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy*, pages 265–300. Springer, 2013.
- [14] R. Anderson and T. Moore. The Economics of Information Security. *Science*, 314(5799):610–613, 2006.
- [15] R. Anderson and T. Moore. Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 367(1898):2717–2727, 2009.
- [16] R. Anderson, T. Moore, S. Nagaraja, and A. Ozment. Incentives and information security. *Algorithmic Game Theory*, pages 633–649, 2007.
- [17] D. Ariely, E. Kamenica, and D. Prelec. Man’s search for meaning: The case of legos. *Journal of Economic Behavior & Organization*, 67(3):671–677, 2008.
- [18] K. J. Arrow. *The Economics of Information (Collected Papers of Kenneth J. Arrow)*, volume 4. Cambridge, Massachusetts: Belknap Press, 1984.
- [19] I. S. Audit and C. A. (ISACA). G41 Return on Security Investment (ROSI), 2010. Available online at www.isaca.org. Last accessed on 06/09/2016.
- [20] M. Baddeley. Information security: Lessons from Behavioural Economics. Working Paper, Gonville and Caius College, University of Cambridge, 2011.
- [21] A. Baldwin, Y. Beres, G. B. Duggan, M. C. Mont, H. Johnson, C. Middup, and S. Shiu. Economic methods and decision making by security professionals. In *Economics of Information Security and Privacy III*, pages 213–238. Springer, 2013.
- [22] J. Baron and J. C. Hershey. Outcome bias in decision evaluation. *Journal of personality and social psychology*, 54(4):569, 1988.
- [23] A. Barth, B. I. Rubinstein, M. Sundararajan, J. C. Mitchell, D. Song, and P. L. Bartlett. A learning-based approach to reactive security. In *Financial Cryptography and Data Security*, pages 192–206. Springer, 2010.

- [24] A. Bashir and N. Christin. Three case studies in quantitative information risk analysis. In *Proceedings of the CERT/SEI Making the Business Case for Software Assurance Workshop*, pages 77–86, 2008.
- [25] J. M. Bauer and M. J. Van Eeten. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10):706–719, 2009.
- [26] D. E. Bell. Disappointment in decision making under uncertainty. *Operations research*, 33(1):1–27, 1985.
- [27] D. E. Bell, H. Raiffa, and A. Tversky. Descriptive, normative, and prescriptive interactions in decision making. *Decision making: Descriptive, normative, and prescriptive interactions*, 1:9–32, 1988.
- [28] D. J. Bem. Self-perception: An alternative interpretation of cognitive dissonance phenomena. *Psychological review*, 74(3):183, 1967.
- [29] S. Benartzi and R. H. Thaler. Myopic loss aversion and the equity premium puzzle. Technical report, National Bureau of Economic Research, 1993.
- [30] Y. Beresnevichiene, D. Pym, and S. Shiu. Decision support for systems security investment. In *Network Operations and Management Symposium Workshops (NOMS Wksp), 2010 IEEE/IFIP*, pages 118–125. IEEE, 2010.
- [31] R. Böhme. Security metrics and security investment models. In *Advances in Information and Computer Security*, pages 10–24. Springer, 2010.
- [32] P. Bordalo, N. Gennaioli, and A. Shleifer. Saliency theory of choice under risk. *The Quarterly Journal of Economics*, 127(3):1243–1285, 2012.
- [33] D. Bouyssou, D. Dubois, H. Prade, and M. Pirlot. *Decision Making Process: Concepts and Methods*. John Wiley & Sons, 2013.
- [34] J. Brenner. ISO 27001: Risk Management and Compliance. *Risk Management*, 54(1):24, 2007.
- [35] D. F. C. Brewer and W. List. Measuring the effectiveness of an internal control system. *Gamma Secure Systems Limited*, 2004.
- [36] D. F. C. Brewer and M. J. Nash. The chinese wall security policy. In *Security and Privacy, 1989. Proceedings., 1989 IEEE Symposium on*, pages 206–214. IEEE, 1989.
- [37] BSI UK. Moving from ISO/IEC, 27001: 2005 to ISO/IEC, 27001: 2013, 2013.
- [38] California State Legislature. S.B. 1386, 2002 Leg., Reg. Sess., 2002.
http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

- [39] C. Camerer and M. Weber. Recent developments in modeling preferences: Uncertainty and ambiguity. *Journal of risk and uncertainty*, 5(4):325–370, 1992.
- [40] C. F. Camerer, G. Loewenstein, and M. Rabin. *Advances in Behavioral Economics*. Princeton University Press, Princeton, NJ, 2011.
- [41] H. Cavusoglu, B. Mishra, and S. Raghunathan. A model for evaluating IT security investments. *Communications of the ACM*, 47(7):87–92, 2004.
- [42] J. L. Cebula and L. R. Young. A taxonomy of operational cyber security risks. Technical report, DTIC Document, Carnegie Mellon University Software Engineering Institute (SEI), 2010.
- [43] G. Charness, U. Gneezy, and A. Imas. Experimental methods: Eliciting risk preferences. *Journal of Economic Behavior & Organization*, 87:43–51, 2013.
- [44] G. Choquet. Theory of capacities. In *Annales de l’institut Fourier*, volume 5, pages 131–295. Institut Fourier, 1954.
- [45] C. C. Chow and R. K. Sarin. Known, unknown, and unknowable uncertainties. *Theory and Decision*, 52(2):127–138, 2002.
- [46] A. Clauset, C. R. Shalizi, and M. E. Newman. Power-law distributions in empirical data. *SIAM review*, 51(4):661–703, 2009.
- [47] C. Colin and L. George. *Behavioral economics: Past, present, future*. Princeton: Princeton University Press, 2004.
- [48] B. Corgnet, P. Kujal, and D. Porter. Reaction to public information in markets: how much does ambiguity matter? *The Economic Journal*, 123(569):699–737, 2013.
- [49] Council of European Union. Council regulation (EU) no 679/2016, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
- [50] S. P. Curley, J. F. Yates, and R. A. Abrams. Psychological sources of ambiguity avoidance. *Organizational Behavior and Human Decision Processes*, 38(2):230–256, 1986.
- [51] C. Derrick Huang, Q. Hu, and R. S. Behara. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, 114(2):793–804, 2008.
- [52] T. Dohmen, A. Falk, D. Huffman, U. Sunde, J. Schupp, and G. G. Wagner. Individual risk attitudes: Measurement, determinants, and behavioral consequences. *Journal of the European Economic Association*, 9(3):522–550, 2011.

- [53] S. Egelman and E. Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2873–2882. ACM, 2015.
- [54] H. J. Einhorn and R. M. Hogarth. Ambiguity and uncertainty in probabilistic inference. *Psychological review*, 92(4):433, 1985.
- [55] D. Ellsberg. Risk, ambiguity, and the Savage axioms. *The Quarterly Journal of Economics*, 75(4):643–669, 1961.
- [56] J. Engle-Warnick, J. Escobal, and S. Laszlo. Ambiguity aversion as a predictor of technology choice: Experimental evidence from Peru. *CIRANO-Scientific Publications 2007s-01*, 2007.
- [57] ENISA. Introduction to Return on Security Investment. Technical report, ENISA, Heraklion, Greece, Dec 2012. Available online at <https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment>.
- [58] M. Ernest-Jones, D. Nettle, and M. Bateson. Effects of eye images on everyday cooperative behavior: a field experiment. *Evolution and Human Behavior*, 32(3):172–178, 2011.
- [59] A. Field. *Discovering statistics using IBM SPSS statistics*. Sage, London, 2013.
- [60] B. Fischhoff, P. Slovic, and S. Lichtenstein. Lay foibles and expert fables in judgments about risk. *The American Statistician*, 36(3b):240–255, 1982.
- [61] D. Florêncio and C. Herley. Sex, lies and cyber-crime surveys. In *Economics of Information Security and Privacy III*, pages 35–53. Springer, 2013.
- [62] F. Foroughi. Information asset valuation method for information technology security risk assessment. In *Proceedings of the World Congress on Engineering*, volume 1, 2008.
- [63] M. Friedman. The use of ranks to avoid the assumption of normality implicit in the analysis of variance. *Journal of the American Statistical Association*, 32(200):675–701, 1937.
- [64] D. Frisch and J. Baron. Ambiguity and rationality. *Journal of Behavioral Decision Making*, 1(3):149–157, 1988.
- [65] V. Garg and J. Camp. Heuristics and biases: implications for security design. *Technology and Society Magazine, IEEE*, 32(1):73–79, 2013.
- [66] D. Geer. Power. law. *Security & Privacy, IEEE*, 10(1):94–95, 2012.

- [67] N. Gennaioli and A. Shleifer. What comes to mind. *Quarterly Journal of Economics*, 125(4):1399–1434, 2010.
- [68] G. Gigerenzer. *Calculated risks: How to know when numbers deceive you*. Simon and Schuster, 2015.
- [69] T. Gilovich, D. Griffin, and D. Kahneman. *Heuristics and biases: The psychology of intuitive judgment*. Cambridge university press, 2002.
- [70] R. Gonzalez and G. Wu. On the shape of the probability weighting function. *Cognitive psychology*, 38(1):129–166, 1999.
- [71] N. Good, J. Grossklags, D. Thaw, A. Perzanowski, D. K. Mulligan, and J. Konstan. User choices and regret: Understanding users? decision process about consensually acquired spyware. *I/S: A Journal of Law and Policy for the Information Society*, 2(2):283–344, 2006.
- [72] L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.
- [73] L. A. Gordon and M. P. Loeb. *Managing cybersecurity resources: a cost-benefit analysis*, volume 1. McGraw-Hill New York, 2006.
- [74] W. T. Harbaugh, K. Krause, and L. Vesterlund. The fourfold pattern of risk attitudes in choice and pricing tasks*. *The Economic Journal*, 120(545):595–611, 2010.
- [75] J. Henrich, S. J. Heine, and A. Norenzayan. The weirdest people in the world? *Behavioral and brain sciences*, 33(2-3):61–83, 2010.
- [76] T. Herath and H. R. Rao. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):154–165, 2009.
- [77] D. Hillson and R. Murray-Webster. *Understanding and managing risk attitude*. Gower Publishing Ltd., Aldershot England, 2007.
- [78] C. A. Holt and S. K. Laury. Risk aversion and incentive effects. *American Economic Review*, 92(5):1644–1655, 2002.
- [79] K. J. S. Hoo. *How much is enough? A risk management approach to computer security*. Working Paper, Stanford University, 2000.
- [80] International Organization for Standardization. ISO Guide 73:2009, Risk Management Vocabulary. 2009.

- [81] International Organization for Standardization. ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management. 2011.
- [82] International Organization for Standardization. ISO/IEC 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Controls. 2013.
- [83] International Organization for Standardization. World distribution of ISO27001 Certifications, 2014. Available online at <http://www.iso270012013.info/news-articles/latest-news/april-2014/world-distribution-of-iso27001-certifications.aspx>.
- [84] C. Ioannidis, D. Pym, and J. Williams. Fixed costs, investment rigidities, and risk aversion in information security: A utility-theoretic approach. In *B. Schneier (Ed.), Economics of Security and Privacy III*, pages 171–191. Springer, 2012. Proceedings of the 2011 Workshop on the Economics of Information Security.
- [85] J. Jackson, N. Allum, and G. Gaskell. *Perceptions of Risk in Cyberspace*. Citeseer, 2005.
- [86] M. E. Johnson. *Managing information risk and the economics of security*. Springer, 2009.
- [87] D. Kahneman. *Thinking, fast and slow*. Macmillan, 2011.
- [88] D. Kahneman, J. L. Knetsch, and R. H. Thaler. Anomalies: The endowment effect, loss aversion, and status quo bias. *The journal of economic perspectives*, 5(1):193–206, 1991.
- [89] D. Kahneman and A. Tversky. Subjective probability: A judgment of representativeness. *Cognitive psychology*, 3(3):430–454, 1972.
- [90] D. Kahneman and A. Tversky. Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, 47(2):263–291, 1979.
- [91] D. Kahneman and A. Tversky. Choices, values, and frames. *American Psychologist*, 39(4):341, 1984.
- [92] J. Keynes. *A Treatise on Probability. Reprint as Vol. 8 of the Collected Writing of J.M. Keynes, 1921*. Macmillan, London, 1971.
- [93] F. H. Knight. Risk, uncertainty and profit. *New York: Hart, Schaffner and Marx*, 1921.
- [94] F. H. Knight. *Risk, uncertainty and profit*. Courier Dover Publications, 2012.

- [95] D. Krantz, D. Luce, P. Suppes, and A. Tversky. Foundations of measurement, vol. i: Additive and polynomial representations. 1971.
- [96] P. Kujal and V. L. Smith. The endowment effect. *Handbook of Experimental Economics Results*, 1:949–955, 2008.
- [97] P. D. Kvam, J. R. Busemeyer, and A. Lambert-Mogiliansky. An empirical test of type-indeterminacy in the prisoner’s dilemma. In *Quantum Interaction*, pages 213–224. Springer, 2013.
- [98] P. K. Lattimore, J. R. Baker, and A. D. Witte. The influence of probability on risky choice: A parametric examination. *Journal of Economic Behavior & Organization*, 17(3):377–400, 1992.
- [99] S. Lichtenstein and P. Slovic. Reversals of preference between bids and choices in gambling decisions. *Journal of experimental psychology*, 89(1):46, 1971.
- [100] P. I. LLC. Cost of Data Breach Study: Australia. 2011.
- [101] C. Locher. Methodologies for evaluating information security investments - What Basel II can change in the financial industry. 2005. In Proceedings of the 13th European conference of information systems, information systems in a rapidly changing economy, ECIS 2005, Regensburg, Germany, 26-28 May 2005.
- [102] G. Loomes and R. Sugden. Regret theory: An alternative theory of rational choice under uncertainty. *The economic journal*, 92(368):805–824, 1982.
- [103] R. D. Luce and J. W. Tukey. Simultaneous conjoint measurement: A new type of fundamental measurement. *Journal of mathematical psychology*, 1(1):1–27, 1964.
- [104] M. J. Machina. ”expected utility” analysis without the independence axiom. *Econometrica: Journal of the Econometric Society*, pages 277–323, 1982.
- [105] M. J. Machina. Choice under uncertainty: Problems solved and unsolved. *The Journal of Economic Perspectives*, 1(1):121–154, 1987.
- [106] M. J. Machina and D. Schmeidler. A more robust definition of subjective probability. *Econometrica: Journal of the Econometric Society*, pages 745–780, 1992.
- [107] T. Maillart and D. Sornette. Heavy-tailed distribution of cyber-risks. *The European Physical Journal B - Condensed Matter and Complex Systems*, 75(3):357–364, 2010.
- [108] J. Marschak. Rational behavior, uncertain prospects, and measurable utility. *Econometrica: Journal of the Econometric Society*, pages 111–141, 1950.

- [109] S. Maximiano. Measuring reciprocity: Do survey and experimental data correlate. Working paper, Krannert School of Management, Purdue University, 2012.
- [110] M. McGuire and S. Dowling. Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report 75, 2013. www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.
- [111] K. Mersinas, B. Hartig, K. M. Martin, and A. Seltzer. Experimental Elicitation of Risk Behaviour amongst Information Security Professionals. *Workshop on the Economics of Information Security (WEIS)*, 2015. Available online at http://weis2015.econinfosec.org/papers/WEIS_2015_mersinas.pdf.
- [112] K. Mersinas, B. Hartig, K. M. Martin, and A. Seltzer. Measuring Attitude towards Risk Treatment Actions amongst Information Security Professionals: an Experimental Approach. *Journal of Cybersecurity*, 2016. doi: 10.1093/cybsec/-tyw009.
- [113] K. Mersinas, B. Hartig, K. M. Martin, and A. Seltzer. Measuring Attitude towards Risk Treatment Actions amongst Information Security Professionals: an Experimental Approach. *Workshop on the Economics of Information Security (WEIS)*, 2016. Available online at http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_22-5.pdf.
- [114] J. M. Miyamoto and P. Wakker. Multiattribute utility theory without expected utility foundations. *Operations Research*, 44(2):313–326, 1996.
- [115] E. Moore and C. Eckel. Measuring ambiguity aversion. Unpublished manuscript. Department of Economics, Virginia Tech. 2003.
- [116] D. Nettle, Z. Harper, A. Kidson, R. Stone, I. S. Penton-Voak, and M. Bateson. The watching eyes effect in the dictator game: it’s not how much you give, it’s being seen to give something. *Evolution and Human Behavior*, 34(1):35–40, 2013.
- [117] M. E. Newman. Power laws, Pareto distributions and Zipf’s law. *Contemporary physics*, 46(5):323–351, 2005.
- [118] J. W. Payne, J. R. Bettman, and E. J. Johnson. *The adaptive decision maker*. Cambridge University Press, 1993.
- [119] W. Pieters. Reve (a, i) ling the risks: a phenomenology of information security. 2009.
- [120] L. PricewaterhouseCoopers and R. Reform. Information security breaches survey technical report. *PricewaterhouseCoopers Report*, 2012.

- [121] J. Quiggin. A theory of anticipated utility. *Journal of Economic Behavior & Organization*, 3(4):323–343, 1982.
- [122] J. Quiggin. *Generalized expected utility theory: The rank dependent model*. Springer Science & Business Media, 1992.
- [123] R. Richardson. CSI Computer Crime and Security Survey, 2008.
- [124] R. Richardson. CSI Computer Crime and Security Survey, 2010.
- [125] I. Ritov and J. Baron. Reluctance to vaccinate: Omission bias and ambiguity. *Journal of Behavioral Decision Making*, 3(4):263–277, 1990.
- [126] H. V. Roberts. Risk, ambiguity, and the savage axioms: Comment. *The Quarterly Journal of Economics*, 77(2):327–336, 1963.
- [127] B. Rohrmann. Risk perception, risk attitude, risk communication, risk management: A conceptual appraisal. *The International Emergency Management Society (Ed.), Global co-operation in emergency and disaster management - 15th TIEMS Conference booklet*, 2008.
- [128] B. Rosner. Hypothesis testing: One-sample inference. *Fundamentals of Biostatistics*, 5:211–271, 1982.
- [129] R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, G. Rogers, and A. Lee. Recommended security controls for federal information systems. *NIST Special Publication*, 800:53, 2005.
- [130] M. Rothschild and J. E. Stiglitz. Increasing risk: I. A definition. *Journal of Economic theory*, 2(3):225–243, 1970.
- [131] R. Sarin and P. P. Wakker. Dynamic choice and nonexpected utility. *Journal of Risk and Uncertainty*, 17(2):87–120, 1998.
- [132] L. Savage. *The Foundations of Statistics, 2nd rev. ed.* New York. Dover, 1972.
- [133] B. Schneier. *Secrets and lies: Digital Security in a Networked World*. New York. John Wiley & Sons, 2000.
- [134] B. Schneier. The psychology of security. In *Progress in Cryptology—AFRICACRYPT 2008*, pages 50–79. Springer, 2008.
- [135] B. Schneier. Worst-case thinking makes us nuts, not safe. Schneier on Security (blog), May 2010. <https://www.schneier.com/essay-316.html>.
- [136] B. Schneier. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015.

- [137] N. J. Schroeder. Using prospect theory to investigate decision-making bias within an information security context. Technical report, Dept. of the Air Force Air University, Air Force Institute of Technology, 2005.
- [138] H. A. Simon. Rationality as process and as product of thought. *The American economic review*, 68(2):1–16, 1978.
- [139] H. A. Simon. Bounded rationality and organizational learning. *Organization science*, 2(1):125–134, 1991.
- [140] P. Slovic, M. L. Finucane, E. Peters, and D. G. MacGregor. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk analysis*, 24(2):311–322, 2004.
- [141] P. Slovic, B. Fischhoff, and S. Lichtenstein. Why study risk perception? *Risk analysis*, 2(2):83–93, 1982.
- [142] M. Spranca, E. Minsk, and J. Baron. Omission and commission in judgment and choice. *Journal of experimental social psychology*, 27(1):76–105, 1991.
- [143] C. Starmer. Developments in non-expected utility theory: The hunt for a descriptive theory of choice under risk. *Journal of economic literature*, 38(2):332–382, 2000.
- [144] R. Steinberger. Proactive vs. Reactive Security, 2003. Available online at <http://www.crime-research.org>.
- [145] S. E. Taylor and S. C. Thompson. Stalking the elusive “vividness” effect. *Psychological Review*, 89(2):155, 1982.
- [146] R. Thaler. Toward a positive theory of consumer choice. *Journal of Economic Behavior & Organization*, 1(1):39–60, 1980.
- [147] R. H. Thaler, A. Tversky, D. Kahneman, and A. Schwartz. The effect of myopia and loss aversion on risk taking: An experimental test. *The Quarterly Journal of Economics*, pages 647–661, 1997.
- [148] H. F. Tipton and M. Krause. *Information security management handbook*. CRC Press, 2003.
- [149] A. Tversky and D. Kahneman. Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, 5(2):207–232, 1973.
- [150] A. Tversky and D. Kahneman. The framing of decisions and the psychology of choice. *Science*, 211(4481):453–458, 1981.

- [151] A. Tversky and D. Kahneman. *Rational choice and the framing of decisions*. Springer, 1989.
- [152] A. Tversky and D. Kahneman. Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, 5(4):297–323, 1992.
- [153] A. Tversky and P. Wakker. Risk attitudes and decision weights. *Econometrica: Journal of the Econometric Society*, pages 1255–1280, 1995.
- [154] V. Verendel. A prospect theory approach to security. Technical report, Department of Computer Science and Engineering, Chalmers University of Technology, 2008.
- [155] J. Von Neumann and O. Morgenstern. *Theory of Games and Economic Behavior (60th Anniversary Commemorative Edition)*. Princeton University Press, 2007.
- [156] F. Wilcoxon. Individual comparisons by ranking methods. *Biometrics Bulletin*, pages 80–83, 1945.
- [157] F. Wilcoxon, S. Katti, and R. A. Wilcox. Critical values and probability levels for the wilcoxon rank sum test and the wilcoxon signed rank test. *Selected Tables in Mathematical Statistics*, 1:171–259, 1970.
- [158] J. F. Yates and L. G. Zukowski. *The anatomy and consequences of ambiguity in decision making*. University of Michigan, Department of psychology, 1975.