Effects of information security risk visualization on managerial decision making

Esra Yildiz
Department of Information Systems,
Westfälische Wilhelms-Universität Münster, Germany
esrayildizz@gmail.com

Rainer Böhme
Department of Computer Science,
Universität Innsbruck, Austria
rainer.boehme@uibk.ac.at

***Abstract* – This paper documents a controlled experiment on the effect of adding a graphical model to a fictitious corporate security decision problem. The control group (*N*=44) saw a textual description, and the treatment group (*N*=41) was presented a graphical representation using the ArchiMate security extension modeling language in addition to the textual description. Besides the security investment decision, indicators of comprehension, risk perception, and decision confidence were measured as dependent variables. Significant positive effects were found for decision confidence and risk perception, but not for the main investment decision and indicators measuring problem comprehension. Two intervening variables, domain knowledge and spatial ability, both derived from the Cognitive Theory of Multimedia Learning, were found to have no significant effect. The experiment presents preliminary evidence from a small sample of educated professionals indicating that visualizations may not have an unconditional advantage over text for decision support in the security domain.**

I. INTRODUCTION

Communicating information security risks is becoming more demanding due to the flood of data produced by information systems, organizational complexities, and technical expert languages. Especially in big organizations, decisions are taken jointly by managers and experts from different domains which requires clean and unbiased understanding of risk. Visualization is one way of communicating security information which could potentially support decision makers by reducing huge data sets into simple visuals. Visual representations are commonly used in finance, marketing and accounting domains. For example, large tables and colorful charts are some of the commonly used visual representations in the day to-day communication between experts and managers about financial risks and their management [1]. Due to the fact that "risk is both very difficult to visualize and extremely challenging to describe" [2], visualization is still not a commonly used tool in the domain of information security management. However, with the increasing technological capabilities, such as graph rendering tools, visual representations are attracting more researchers as well as being more preferred in security management activities on the organizational side. The recent information security visualization studies are progressively focusing on visualization of data analysis, data analytics and event identification aiming at mostly preventing attacks and detecting vulnerabilities [3]. Despite the growing interest into security visualization research, few researchers have seriously examined the impact of visualization in the information security management context. In their recent study, Hall et al. [4] explore the current roles of information security visualizations and conclude that visual representations improve critical thinking and help the stakeholders in risk assessment phase. Labunets et al. [5] compare tabular and graphical representations to find out which visual is a better fit when communicating information security risks. Additionally, Li et al. [6] offer a novel approach which enables the formulation of a visual vocabulary to represent any kind of complex security model.

Our research explores the effect of graphical representations on information security decision making. It builds on Mayer's [7] Cognitive Theory of Multimedia Learning (CTML) in the hypothesis formulation phase. In this study, visualization refers to graphical representations in the form of conceptual models. The principal research question addressed in this study is:

"Does model based visualization of security properties affect decision making in the information security domain?"

Since decision making is a complex cognitive process, which is difficult to assess empirically, we decomposed it into the following set of measurable phenomena: comprehension, risk perception, risk taking behavior, and decision confidence.

Five hypotheses (and one sub-hypothesis) were postulated to examine the effect of visualizing security properties integrated in the IT architecture. Primary data was collected using a tailored online questionnaire in a controlled experimental design. We have created an imaginary case and modelled the business and IT architecture with its security properties (see Appendix). To identify the effect of a visual model, a randomly assigned half of the participants received only a textual description of the case, and the other half received the textual description along with a graphical model. From a convenience sample of 85 subjects, we observed that visualization of security properties integrated with

EuroUSEC '17, 29 April 2017, Paris, France

http://dx.doi.org/10.14722/eurousec.2017.23010

the system architecture does affect the decision outcome somewhat, but much less than hypothesized. We find no effects on the comprehension and risk taking behavior of the participants, and small but statistically significant positive effects on their decision confidence and risk perception.

II. Theory and Related Work

A. Risk Perception in the Information Security Domain

The manner in which decision makers perceive the information security risks, shape what decision they make to secure an organization and its stakeholders. The mismatch between reality and perception of information security risk could lead managerial decision makers to take misguided decisions which can reduce the strength of a company's security posture. Protection Motivation Theory (PMT) suggested by Rogers [8] is a widely accepted and adopted theoretical perspective when explaining and assessing risk perception. PMT explains how people are motivated to protect themselves from a risky situation with two principal drivers: threat appraisal and coping appraisal. Threat appraisal is related to perceived severity and susceptibility of a threat event, reflecting how serious the event is. While perceived susceptibility is the likelihood of being exposed to a threat, perceived severity is the effect of potential consequences posed by the threat [9]. Coping appraisal is related to response efficacy and self-efficacy, expressing how individuals respond to a threat event. While self-efficacy can be described as the confidence in being able to undertake the recommended behavior, response efficacy is associated with executing recommendations to avoid the threat event. Together with those constructs, it is possible to assess the perceived risk or behavioral intentions to avoid specific risks. According to Rogers et al. [10], PMT is an essential cognitive rationalization of protective behavior.

Another dimension of risk perception materializes in risk taking behavior. It is defined as an individual's preference of a high uncertain payoff over a lower payoff with certainty. For example, an individual without risk taking behavior would keep his/her money in a bank with a standard interest rate, while one with risk taking behavior would invest in a lottery. Especially the relation between risk perception and risk taking behavior is investigated by the health behavior theories examining the hypothesis of perceived vulnerability being the major motivational source of precautionary behavior [11]. This hypothesis has been supported by a number of studies providing indications that perceptions of vulnerability are positively correlated with different precautionary behaviors [12], [13].

B. Decision Making and Risk Communication

Depending on the role of security in an organization, information security decisions may be associated with topics such as IT investment, security policy and procedure definitions, staffing, security governance or disaster recovery [14]. In many organizations, information security decisions involve variety of trade-offs between productivity and security, cost and benefit or privacy and convenience. Such multifactorial decision making has been investigated in the security economics literature. For example, Beresnevichiene et al. [15] proposed a method to support information security investment decision makers with systems modeling and validated it with a case study. Baldwint et al. [16] conducted a controlled experiment on how economic framing can influence security professionals' way to make and justify decisions. In particular, the second study established a link between prescriptive security investment models and risk communication.

Risk estimates are particularly hard to understand for decision makers who are not experienced in understanding the source of risk and the methods used for quantification. In these cases, the risk communication language can be a substantial barrier. If the way risk information is structured and motivated does not match among different stakeholders, then risk communication inevitably fails. A study exploring the reasons of communication problems between security professionals and executives concluded that risk communication is often hindered due to stacked information and a presentation that is not easily understood by non-technical managers [17]. Against this backdrop, risk management, decision making, and risk communication arguably require effective and contemporary communication instruments. One possible instrument for the improved communication and decision support can be 'visualization'. If security risks are represented appropriately, visualization can bring various cognitive and communicative advantages for decision makers.

C. Visualization in the Information Security Domain

Visualizations can have various advantages during sense-making, exploration, problem solving, decision making and communication of complex ideas. According to Sarlin [18], "visualization can be seen as a type of cognitive support or amplification that strengths or weakens human perception". As Bettman and Kakkar [19] stated, by changing the presentation of information, visualization tools can have different implications for both decision processes and outcomes. For instance, visualization can enable certain information to stand out more than other, or make it easier to observe patterns and exceptions, which could eventually improve decision quality [20]. On the other hand, visualizations tend to lead to biases in decision making, if the information is not structured well or does not provide a complete awareness related to the whole data set.

Visualizations are widely used in a variety of application domains such as finance, accounting, journalism and marketing. However, visualization in the information security domain is not a common topic in organizations, due to the fact that security is hard to visualize in nature and security experts are reluctant to incorporate visual representations in their daily work [21]. In general, organizations are increasingly pooling huge amounts of data regarding the state of their information security. Therefore, methods such as advanced modeling and simulation are being more essential for classifying threats, specifying attack mechanisms, verifying countermeasures, and monitoring the consequences [22]. Both in the academia and practice, information security visualizations are largely focused on the topics of data analysis, event identification, event analysis and situational awareness [23]. Such visualizations usually center on the processes, such as network monitoring and

incident management, where visual representations are useful in terms of anomaly detection and revealing patterns.

Visualizations in information security management can be used in different formats for various tasks. For example, Key Performance Indicators (KPI) are one of the common instruments used in the security domain to evaluate the success of a security program or an activity. Some indicators have been used to rationalize risk in terms of monetary value, such as Return on Security Investment (ROSI), Annual Loss Expectancy (ALE), Net Present Value (NPV), and Value at Risk (VaR) [24]. Dashboards, plotted diagrams, benchmarking graphs and histograms are commonly used examples of visual representations for such indicators. Furthermore, in information security management, visualization comes into sight of attack modelling or threat modelling in the product design phase.

In this study, we focus on visualization with modelling languages which support the effort of formalizing security. Conceptual models are convenient tools for decision makers, enabling them to abstract and capture different aspects of information systems in diagrammatic fashion [25]. The aim of conceptual security modelling is to display how security concepts (i.e. vulnerabilities, countermeasures) can be integrated into the architecture. It thus supports decision makers by demonstrating the dependencies between sources of risk, controls, and the environment. Several security modelling languages or security extensions to existing languages have been developed to incorporate information security in models. UMLsec, Secure Tropos and Misuse cases are some of the prominent categories of security modelling approaches built on well-established frameworks [26], [27], [28]. Another security modelling extension is based on the ArchiMate modelling language, which is a widely-adopted enterprise architecture modelling language in the industry. Throughout the empirical part of this study, a specialized version of ArchiMate's risk and security overlay [29] is used to test the effect of visualization on decision making. The aim of this overlay is to provide enterprises with a medium to manage risks in a more integrated fashion.

D. Decision Making and Information Representation

There has been considerable research addressing the effectiveness of information visualization on decision making performance [30], [31], [32]. According to Tegarden [32], in some circumstances, representing information visually enables decision makers to amplify their perceptual processes and support their information exploration capabilities. However, research conducted by DeSanctis [33] and Vessey [34] shows that information visualization might not be useful in all situations, meaning that the effectiveness of the visualization format depends on the decision task.

The layered reference model of the brain (LRMB) developed by Wang et al. [35] tries to explain the cognitive processes of human intelligence. According to the model, meta-cognitive processes, such as abstraction, categorization, search, memorization, and knowledge representation, are grouped in a sub layer and used by the higher cognitive processes. In the higher layer of the model, high cognitive processes, such as learning, reasoning, problem solving, and decision making, are classified. We can derive from the LRMB model that the success of the higher cognitive functions strongly depends on the lower cognitive functions. Furthermore, the relationship between decision making and other meta-cognitive functions, such as comprehension, memory, and abstraction, shows that there is a strong relation between the decision making process and the comprehension, search, memorization, and presentation processes [36]. In the light of this information, it can be stated that visualization may increase the decision quality and performance as it decreases the search time and supports the memorization process by creating mental models.

Another effect of visualization on decision making can be observed on the dimension of decision confidence. The term decision confidence can be summarized as the belief in the quality of decision [37]. Decision confidence is crucial, especially in the implementation phase of the decision, because over-confidence in a poor decision or under-confidence in an effective decision can result in disasters [38]. Some of the different factors influencing the level of decision confidence are the characteristics of information, decision aids, decision maker, and the given tasks [39].

Visualizations offering various cognitive benefits can influence decision confidence as well. According to Koriat et al. [40], the quality of information supporting the decision making is directly related to the level of confidence. Schwenk [41] posits that when the quantity of the available information is increased, people become more confident as they can generate more justifications. Furthermore, findings reveal that "vividness affect perception of information quality which influences the confidence on decision making" [42]. On the other hand, decision confidence can influence interpretation, perception, and ultimately the resulting judgments. Phillips, Prybutok, and Peak [43] point out the correlation between decision confidence and perceived expertise, where higher decision confidence can cause oversight and incorrect interpretation of the information, as individual's preconceptions would overshadow the information presented to them.

So far, little is known about the effect of visual representations on changing risk taking behavior. For example, the study conducted by Stone at al. [44] shows that individuals are more willing to pay for an improved product when graphics (stick figures, bar graphs, and asterisks) are added near to a numerical presentation. Lipkus and Hollands [45] also state that similar other graphs, such as histograms and facial diagrams, may affect perceived risk and eventually lead individuals to make risk reluctant choices. To the best of our knowledge, no literature studies the relationship between information security risk taking behavior and visual representations. However, in the light of the information from other research domains, it is reasonable to conjecture that such a relation exists.

E. CTML Theory

Developed by R.E. Mayer over the last 30 years [7], [46], [47], the CTML combines the science of learning and the science of instruction in order to explain how to make best use

of multimedia representations in learning by reducing the cognitive load for the learner. The theory is constructed on three basic sets of assumptions by making use of three different theories. Those assumptions are: dual channel processing, limited capacity, active processing.

Firstly, the dual channel processing assumption suggests that individuals have two separate information processing channels for visual and auditory information. Those two channels complement each other, in a fashion that receiving concurrent information through multiple channels enhances the overall recall, compared to receiving information through only one channel [48]. Secondly, the limited capacity assumption is based on the cognitive load theory [49], [50], which suggest that cognitive load is cumulative in nature and individuals have limited capacities when processing information. Finally, the active processing assumption is based on constructivist learning theory [51], which suggest that meaningful learning occurs when learners actively select relevant information, organize it into coherent representations, and integrate it with the knowledge stored in the long-term memory [47]. The three sets of assumptions, the CTML, enabled Mayer to outline several design principles to support designers and teachers to create effective multimedia representations. The proposed principles are; multimedia, contiguity, coherence, modality, redundancy, and individual differences [7]. Only the relevant ones for this study are examined.

The multimedia principle is based on the assumption that individuals learn better when using two modes of representation (i.e. from words and graphics) rather than one (i.e. from words alone). Mayer captures the multimedia effect in his study where students who read a text including illustrations placed near the corresponding words suggested 65% more useful solutions to a problem-solving test than did students who solely read the text [54], [46]. The individual differences principle is based on the assumption that the multimedia design principles have stronger effects for low-knowledge learners than for high-knowledge learners, and for learners with high spatial ability rather than for learners with low spatial ability [53].

Knowledge effect: Mayer's study shows that students who have less prior knowledge tended to show stronger multimedia effects than students who have high levels of prior knowledge [54], [55]. This result can be explained by the CTML in that students with high prior knowledge may be able to generate their own mental images, hence they do not need to make use of the visuals. Whereas, visualizations are helpful for students with low prior knowledge in terms of establishing connections between the visual and verbal representations, and reducing cognitive load.

Spatial ability effect: Mayer's study shows that students with high spatial ability showed a stronger multimedia effect than the students with low spatial ability [55]. This result can be explained by the CTML theory in that individuals with high spatial ability are able to hold the visual image in visual working memory. Thus, they are more likely to build connections between visual and verbal information, which is required to benefit from the contiguous presentation of words and pictures [53].

Readers should be reminded that multimedia presentation is defined by Mayer [7] as "the presentation of material using both words (written or spoken text) and pictures". Unlike the popular definition of "multimedia", Mayer's definition is neither referring to the media (such as computers or television) used to deliver the message nor to the presentation mode (such as animation); rather, he refers it to the sensory mode message recipients use to process the presented information [56]. Since conceptual models are composed of words and graphics, the model-based representation fits well with the Mayer's notion of multimedia. Moreover, as conceptual models are visual representations comprising words and graphs, CTML is arguably the theory of choice when generating, testing and explaining the outcomes of the first two hypotheses explained in the next section.

III. Empirical Approach

This section first derives the hypotheses from the theoretical background. Following that, the research method, procedure, and the measurement of key constructs are described.

A. Hypotheses

In order to answer the research question of this study, the following hypotheses are postulated.

The first hypothesis is based on the multimedia principle of the CTML, which suggest that individuals learn better from words and graphics than from words alone. Hence, including a relevant conceptual model near a textual description of a security case should reduce the tendency of cognitive overload and increase the comprehension of the information being presented to decision makers.

H1: The addition of a conceptual model near a textual description improves the comprehension of the decision maker.

The second hypothesis is based on the individual differences principle of CTML, which suggests that multimedia effects are stronger for individuals who have low knowledge than the ones with high knowledge; and for good spatial learners than for bad spatial learners [7]. We formulate two sub-hypotheses, H2.1 and H2.2.

H2.1: Compared to the individuals with high security domain knowledge, the individuals with low security domain knowledge improve the comprehension score more when a conceptual model is added near a textual description.

H2.2: Compared to the individuals with low spatial ability, the individuals with high spatial ability improve the comprehension score more when the conceptual model is added near a textual description.

Based on the explained theoretical background on the decision confidence phenomenon in Section II.D, visual representations are expected to increase the decision confidence in the information security domain.

H3: The addition of a conceptual model near a textual description increases the decision confidence of the decision maker.

As discussed in Section II.D, risk perception is a complex cognition and can be influenced by many different factors, such as individual judgements and evaluations. As the graphical representations influence cognition, we can argue that if the complex reality of information security is communicated in terms of graphical representations, the deviation between perception and the reality may decrease. Hence, visualizations might improve the risk perception of the decision makers.

H4: The addition of a conceptual model near a textual description increases the risk perception of the decision maker.

Based on the explained theoretical background on the relationship between risk perception phenomenon and risk taking behavior in II.A, increasing risk perception can influence individuals to take more precautious decisions. Mainly, when the severity and the likelihood of an information security risk is considered to be high, individuals should feel fear and decide on less risky portfolios. As our assumption is that visualization can induce perception of risk, we can expect a decrease in risk taking behavior if an individual encounters well-structured visualizations. If the visual representations affect the way individuals imagine an uncertainty or risk, it may also alter their precautionary behavior. According to Lipkus and Hollands [45], visual representations appeal emotions and arouse thoughts and feelings regarding the experiences or imagined negative events. Building on top of this assumption, we can expect graphical models to influence imagination, hence negatively affecting risk taking behavior in the information security domain as well.

H5: The addition of a conceptual model near a textual description lets decision makers choose more cautions alternatives.

B. Research Method

To measure the effect of visualization on the defined notions – decision confidence, comprehension, risk perception and risk taking behavior – a controlled experiment was conducted. An online questionnaire, with the capability of randomly assigning participants to two different groups, was sent to various security mailing lists as well as shared via social media. The targeted participant characteristics were individuals with business, information security, or IT backgrounds. To explore the impact of the visualization in a more practical and realistic setting, we created a written case scenario of an attack against an online store inspired by real-world security breaches. According to the design, half of the participants received a security case incorporating a system description and related security aspects (e.g. vulnerabilities, countermeasures) in a textual form *including* a conceptual model attached near the text. While the other half of the participants, namely the control group, received only the textual description of the security case with the system description and security aspects. The intention of this set-up was to identify the influence of the model by holding everything constant in each group except the presence of the model. The conceptual model was modelled with the risk and security overlay of the ArchiMate [29] language and was designed to reflect the same information as the textual description in a diagrammatic fashion. We have chosen the ArchiMate modeling language as it is already being used as a commercial product and hence closer to practice than purely academic visualizations.

The online questionnaire was divided into several sections; demographic questions, security case, comprehension, risk perception and behavior questions, post-survey questions, and spatial ability questions. These sections were presented to the subjects in a sequence of web pages and participants were not permitted to navigate to the previous pages. The reason for placing the spatial ability questions on the last page was to limit the cognitive load on participants and to keep them from quitting the survey at an earlier point.

C. Procedure and Measurement of Key Constructs

The procedure began with asking simple demographic questions and continued with a short informative description of DDoS attacks, aimed at training the participants regarding the security case. After that, a security case involving a possible DDoS attack against a fictitious company was displayed. Along with general explanations on the imaginary company profile, a system description including business processes, technical architecture as well as the related security aspects, such as vulnerabilities and mitigation options, were expressed on a high level.

Comprehension measure: After reading the case, on the next page, participants were asked to answer five case-related comprehension questions. These questions were constructed in a fashion that could be answered directly from the textual description or the graphical model, in order to assess if the visualization enables participants to keep the images in their short-term memory. The comprehension measure was given by the sum of correct answers.

Risk perception measure: After the comprehension questions, participants were asked to answer five questions aimed at revealing their risk perceptions regarding the DDoS attack case. To measure the risk perception, core constructs of PMT theory, namely perceived severity and perceived susceptibility notions, were used. The risk perception questions were created by drawing on the study from Johnston and Warkentin [57], who measured risk perception by using a combination of threat severity and threat susceptibility items. Each question was rated on a five-point rating scale ranging from 1 (strongly disagree) to 5 (strongly agree) and their sum was used for the measurement. Two of the questions were placed as mirror questions to identify response patterns. We have examined the correlation matrix (see Appendix) and observed a strong response pattern, meaning that most of the respondents were not able to identify the negation. Therefore, we decided to exclude the mirror questions for the validation phase.

Decision confidence measure: After the investment decisions were made, participants were asked three questions to

express their decision confidence with regard to the investment they have made earlier. A five-point rating scale ranging from 1 (strongly disagree) to 5 (strongly agree) was used. For the measurement, the scale rating was aggregated. Furthermore, among the three decision confidence questions, one of them was constructed as a 'mirror' question. This approach was thought to be useful to capture response patterns, if there were any. In this case, we observed that around one quarter of the respondents understood the mirror question wrong and ignored the negation. However, we decided to include the mirror question in the validation phase as its correlations observed to be not too low (see Appendix).

Risk taking behavior measure: Following the risk perception questions, two information security investment questions were asked to measure the risk-taking behavior of the participants. A trade-off between the cost and benefit was given, and participants were expected to make a decision between a solution with high cost/low risk and a solution with low cost/high risk or neither of them. A value has been assigned to each question and the sum of those values was used for the measurement. Individuals who scored above the median were recorded as high risk takers and the others were recorded as low risk takers.

Individual differences measure: To measure the domain knowledge of the participants, they were asked to rank their domain knowledge on business, IT and IT security on a seven-point rating scale with response options ranging from "none" to "excellent". Individuals who marked 'excellent' and 'very good' were recorded as 'participants with high knowledge' on the IT security domain and who marked 'none' and 'poor' were recorded as 'participants with low knowledge'. In the final section of the questionnaire, three questions were asked to measure the participant's visual spatial ability. Individuals who scored above the median were recorded as high spatial ability learners while the others were recorded as low spatial ability learners. In order to avoid loading respondents cognitively, these questions were located at the end of the survey labelled with a note indicating that those questions were optional.

For reproducibility, questions and scales are included in the Appendix.

D. Pretest

In order to improve external validity and to limit ambiguity in the online questionnaire, we have conducted a pretest with a handful of respondents from the target group. The length of the questionnaire was a common concern leading us to leave out some questions. The spatial ability questions were somewhat discouraging to respondents who were willing to share their domain knowledge, but not wanting to feel like in an exam. We replaced some of the spatial ability questions and displayed them at the end of the questionnaire by marking them as "optional". Furthermore, some levels of ambiguity were observed on the security investment decision making questions. As some pretesters were not experienced in making security investment decisions, there was a level of misinterpretation, which we tried to remediate with adjusted wording. In general, pretesters reported that they found it easy to interpret the graphical model. They also thought the text appropriately reflects the system and security properties together.

IV. RESULTS

Between April and May 2015, a total of 186 participants viewed the questionnaire, leaving us with a final data set of 85 usable responses. Approximately 81 percent of the respondents were male and most of the participants (48%) were between 20 and 29 years old. As for the level of education, 56 percent completed a master's degree as their highest level of education, followed by the bachelor's degree with 33 percent. A heterogeneous level of experience was identified; 30 percent being mid-level, 25 percent being senior level and 24 percent being entry level with the bulk (42%) working in a large organization. 53 percent identified their IT background and 36 percent their IT security background as high by marking 'very good' and 'excellent' on the scale. The results showed that most of the participants (23%) were from IT sector, followed by the education and energy sectors.

To reveal participant's attitudes to cyber security and experience of cybercrimes information, we made use of questions taken from the Eurobarometer study [58]. A clear majority (80%) of the respondents reported a high level of concern regarding cyber security crimes, but most of the participants have not fallen victim of an online crime.

Furthermore, as a data quality check, we wanted to reveal participants' opinions towards the graphical model. Participants who saw the conceptual model along with the textual description were asked to evaluate the benefit of the conceptual model in terms of supporting their understanding. A significant number of respondents (67%) reported that the existence of the model supported their understanding of the security properties of the presented case. Participants were also asked to reveal their opinion with regards to relationship between decision making and conceptual model visualization, in both groups, respondents were in favor of the idea that conceptual models can improve decision making. Additionally, in the questionnaire, participants who saw the conceptual model near the textual description were also asked to indicate their level of expertise of the ArchiMate modelling language. The results showed that a substantial part (41%) of participants was not aware of the existence of the ArchiMate modelling language. And half of them seemed to be undecided on their level of understanding regarding the conceptual model.

Table 1: Descriptive statistics for all the dependent variables

		Model + text				Text only			
Dependent Variables	***NQ***	***M***	***CI***	***N***	***SD***	***M***	***CI***	***N***	***SD***
Comprehension; number of correct answers; (min:0, max: 1)	5	3.85	±0.42	41	1.35	3.86	±0.37	44	1.23
Decision confidence; sum of confidence rating; (min: 0, max: 5)	3	11.2	±0.61	41	1.95	9.98	±0.78	44	2.57
Risk perception; sum of perception rating; min: (0, max: 5)	3	11.6	±0.40	41	1.27	10.8	±0.52	44	1.72
Risk taking behavior; sum of solution alternatives[1]; (min: 0, max: 2)	2	2.78	±0.34	41	1.08	2.84	±0.30	44	1.00

Note: NQ: number of questions; M: mean; CI: 95% confidence interval; N: sample size; SD: standard deviation; 1: low cost/high risk solution: 2, high cost/low risk solution: 1, none of the solutions: 0

A. Comprehension Test

Descriptive statistics on the comprehension score are given in Table 1 and visualized in Figure 1. To understand the effect of displaying a conceptual model on comprehension of the participants, we used negative binomial regression analysis. Compared to the text-only group, the comprehension score decreased marginally when the graphical model was displayed near the text. However, the effect was not statistically significant (Table 2).

Table 2: Regression for predicting the effect of visualization on comprehension

Dependent Variables	***B***	***SE B***	***df***	***p***
Comprehension score				
Intercept	1.35	.169	1	.000*
Model + text	.003	.243	1	.992
Text only	0	-	-	-
Wald Chi Square (X^2) = 63.854				

Note: * $p < .05$; N=85; *B*: unstandardized coefficient; SE: standard error; df: degrees of freedom; *p*: *p*-value

B. Individual Differences Test

We used two-way analysis of variance (ANOVA) to understand the effect of the graphical model on the comprehension score of the respondents with low and high domain knowledge as well as with good and bad spatial ability. From the data (Table 3), it can be derived that prior domain knowledge is significantly (p-value=0.018) correlated with the comprehension score. However, the presence of the model did not make a significant difference on the comprehension score of the participants with low knowledge. The hypothesized effect, visualization being a catalyst for the participants with low knowledge to have a better comprehension score (H2.1), is not supported. As for the effect of the graphical model on good and bad spatial learners, we observed that comprehension is positively correlated with the spatial ability score. Contrary, the presence of the model did not make a significant difference on the comprehension of the high spatial learners. There is no empirical support for H2.2.

Table 3: Two-Way ANOVA of knowledge and spatial ability effect

Dependent Variables	***df***	***SS***	***MS***	***F***	***p***
Comprehension score					
Interaction (K x V)	2	1.23	.617	.399	.672
Knowledge (K)	3	16.4	5.47	3.35	.018*
Visualization (V)	1	.031	.031	.020	.888
Comprehension score					
Interaction (S x V)	1	1.08	1.084	.660	.419
Spatial ability (S)	1	5.51	5.511	3.354	.071
Visualization (V)	1	.002	.002	.001	.971

Note: * $p < .05$; N= 84; mean substitution was performed for the respondents who did not fully answer all of the questions

C. Decision Confidence Test

According to the data set shown in Table 1 and Figure 1, decision confidence is higher when the graphical model is displayed. To understand the influence of the graphical representation on the decision confidence, a one-way ANOVA was used (Table 4). We found a significant relationship between the decision confidence and the visual representation, with *p*-value 0.014. When the conceptual model is located near the textual description, participants' decision confidence regarding a risky investment was increased (see Table 1 and Figure 1). While this lends support to H3, the effect size was at the upper end of "small" according to the measure of Glass' delta (Δ=0.49), making it difficult to evaluate the meaningfulness of this effect. It was at the lower end of "medium" according to the more common criterion, Cohen's *d* (d = 0.55). For perspective, subjects in the treatment group on average selected about one step "more confident" on one out of three 5-step rating scales, than subjects in the control group (see Appendix for scales). Besides the direction, it is hard to translate this difference into practice or evaluate its economic significance. To rule out that a possible violation of assumptions required by the parametric tests caused spurious results, we also computed a non-parametric Mann-Whitney test. Its *p*-value of 0.012 confirmed robustness.

D. Risk Perception Test

Descriptive statistics on the risk perception score are given in Table 1 and visualized in Figure 1. In order to measure the effect of visualization on risk perception, a one-way analysis of variance was used. The resulting ANOVA (Table 4) shows that there is a statistically significant (p =0.019) effect of the model representation on the risk perception. This supports H4. Also here, the effect size was at the upper end of "small" (Δ=0.46, d=0.52), and the Mann-Whitney test confirmed robustness (p =0.018). The practical interpretation is subject to the same limitations as mentioned in the previous section for decision confidence.

Table 4: One-way ANOVAs on decision confidence, risk perception and risk taking behavior

Dependent Variables	*df*	*SS*	*MS*	*F*	*p*
Decision confidence					
Between groups	1	33.26	33.26	6.34	.014*
Within groups	83	435.0	5.242		
Total	84	468.3			
Risk perception					
Between groups	1	13.35	13.35	5.73	.019*
Within groups	83	193.3	2.33		
Total	84	206.7			
Risk taking					
Between groups	1	.019	.019	.07	.783
Within groups	83	20.73	.250		
Total	84	20.75			

Note: *p < .05; N= 85; df: degrees of freedom; SS: sum of squares; MS: mean sum of squares; F: f-statistic; p: p-value; mean substitution was performed for the respondents who did not fully answer all of the questions

E. Risk Taking Behavior Test

Descriptive statistics on risk taking behavior are given in Table 1 and visualized in Figure 1. One-way ANOVA was used to examine the relationship between risk taking behavior and the model representation as well. According to the ANOVA results (see Table 4), there was no statistical significant effect. Therefore, H5 is not supported.

V. DISCUSSION

Table 5 summarizes all hypotheses and their empirical support. The first hypothesis was based on the CTML theory, predicting a potential improvement on comprehension when the visual representation is displayed near the text. However, no improvement was observed and this hypothesis was rejected. The reason for this outcome could be due to the nature of the comprehension questions. It is possible that participants did not require to put high effort into building connections between the model and the textual description as the questions appeared to be rather simple. This might have caused a lack of significant difference in the comprehension outcomes between the two groups. Another explanation of this outcome could be lack of task fit. Cognitive fit theory [59] states that task and the representation should have a natural fit in order to enable more effective and efficient communication and decision making. It could be the case that modelling security properties graphically is not an effective way of supporting comprehension of the individuals regarding the security case.

The second hypothesis was based on the individual differences principle of the CTML, which predicted that visualization improves comprehension more strongly for individuals who have low knowledge than for the ones with high knowledge; and for good spatial learners than for bad spatial learners. Both sub-hypotheses predicted interaction effects, which in general are more difficult to identify in small samples than direct effects. This may explain the result that the presence of the graphical model did not make a statistically significant difference in the sub-groups; neither between the participants with high and low visual spatial ability nor between the participants with high and low prior domain knowledge. As stated before, the reason of these outcomes could be due to the characteristics of the comprehension scores. Furthermore, according to Mayer and Sims [55], people with high spatial ability devote more cognitive resources when building referential connection between visual and verbal representations. For *H2.2*, we can argue that high spatial ability respondents did not require to put much effort into building connections between the graphical model and the textual description. Additionally, in order keep the questionnaire short, we could incorporate only three spatial ability questions and those questions were labeled as optional. Perhaps this setting prevented us from measuring the exact spatial cognition of the respondents, and hence might have caused us to reject the spatial ability hypothesis.

The third hypothesis was based on the assumption that when the graphical model and the text are displayed together, respondent's decision confidence in making an investment under uncertainty increases. This hypothesis was validated. The presence of the graphical model might have reduced the amount of cognitive load required by the decision maker and contributed to improve his decision confidence. Alternatively, the quality and quantity of information [40], [41] might have increased with the visualization and stimulated the decision confidence. According to O'Reilly [60], information abundance generally induces higher confidence for decision makers. Furthermore, this finding aligns with research on information seeking intention [61]: When the visual format of information is presented, users are not led to seek information, whereas when information is presented only in textual format, users are led to seek additional information.

The fourth hypothesis was generated on the assumption that the respondent's risk perception increases when the graphical model is displayed. This hypothesis was validated. We explain this outcome with visualization being an effective tool for risk communication. The conceptual model might have simplified the understanding of the risky situation, which might have led participants to imagine the imaginary attack and its effect on the system more easily. Furthermore, warning icons located on the model components might have influenced the

Table 5: Overview of hypotheses and results

Hypotheses	***Test Type***	***Statistics***	***Result***
H1: The addition of a conceptual model near a textual description improves the comprehension of the decision maker.	Negative binomial regression analysis	$p = .992$	rejected
H2.1: Compared to the individuals with high security domain knowledge, the individuals with low security domain knowledge improve the comprehension score more when a conceptual model is added near a textual description.	Two-way ANOVA	$p = .672$	rejected
H2.2: Compared to the individuals with low spatial ability, the individuals with high spatial ability improve the comprehension score more when the conceptual model is added near a textual description.	Two-way ANOVA	$p = .419$	rejected
H3: The addition of a conceptual model near a textual description increases the decision confidence of the decision maker.	One-way ANOVA	$p = .014$ $\Delta = 0.49$ $d = 0.55$	supported
H4: The addition of a conceptual model near a textual description increases the risk perception of the decision maker.	One-way ANOVA	$p = .019$ $\Delta = 0.46$ $d = 0.52$	supported
H5: The addition of a conceptual model near a textual description lets decision makers choose more cautions alternatives.	One-way ANOVA	$p = .783$	rejected

perception of the respondents aligned with the study of Egelman et. al [62]. Hence, the resulting feelings might have facilitated increased risk perception. For the future research, we suggest eliminating any strong warning signs to isolate effects caused by the strong signs.

With the last hypothesis *(H5)*, we predicted that presenting a graphical model along with the text would influence participants to make more cautious decisions regarding a risky investment. However, this hypothesis was rejected. We assumed that increasing risk perception would provide behavioral change towards taking precautions, however aligned with the research conducted by Weinstein [63], [64], respondents are rather optimistic regarding the imaginary attack. They might have thought the vulnerability is not severe, or it would not occur in the case of the fictitious company. This outcome can also be explained by the Adoption Process Model, which suggest that "changes in intention will occur only when a change in behavior is perceived to be effective and the problem is perceived to be severe enough to warrant action" [65]. From another perspective, the reason for this outcome could be linked to the improved decision confidence, which might have encouraged the risk taking behavior of the respondents. This result is in line with several prior studies suggesting that overconfident individuals tend to make risky financial predictions that are not assured by the available information [66], [67]. This finding provides some evidence that increased confidence may influence risk taking behavior in the information security domain as well.

Figure 1: Dotplots of dependent variables grouped by treatment (Model + text, N=41) and control (Text only, N=44), group means, and 95% confidence intervals. Jitter has been applied to separate identical values.

A. Limitations

Although this research has reached its aims, there are some inevitable limitations. First, due to economic constraints, this research was conducted only on a small sample with strong over-representation of educated and male participants compared to the general population. A larger sample would have narrowed the confidence intervals and, consequently, allowed us to statistically detect effects of smaller sizes. A more representative (i.e., less biased) sample of the relevant population would have improved the generalizability of our results. Furthermore, as we aimed at measuring many different decision aspects, it was unavoidable to design a lengthy and complex questionnaire. That is the main reason why although the online questionnaire reached a high number of people, not everyone was interested in completing it. Another significant limitation is the focus on a single case to test the hypotheses. Potentially, a superior generalization could be done if multiple cases incorporating different security subject areas were studied sequentially or independently. The same can be said for the choice of a single visualization technique.

Since research in this sub-field is relatively new, its theory is underdeveloped. We had to resort to more general theories of human behavior or ad hoc assumptions when deriving our hypotheses. For example, even though most of the literature claims that visualization can improve decision making under uncertainty, little research actually supports this with evidence. Therefore, it is still not obvious how much benefits security experts and managers can get from visual representations.

VI. CONCLUSION

The main objective of this research was to investigate how visualization of security properties impacts managerial decision making in the information security domain. The research was set out from the idea of visualization technologies providing broad capabilities for supporting decision makers in business, finance, and marketing domains. Thus, we were curious to study the effects in the context of information security decision making. As decision making is a far-reaching concept, it was abstracted into several smaller notions for a systematic empirical experiment. Notions of comprehension, risk perception, risk taking behavior, and decision confidence were studied to deduce a conclusion on the relationship between decision making and visualization. The result of the online experiment showed that visualization has no measurable impact on the comprehension and risk taking behavior, and a small positive impact on decision confidence and risk perception. We argued that the presence of a conceptual model might have reduced the amount of cognitive load required by the decision maker, and thereby contributed to improve his/her decision confidence. Alternatively, the quality and quantity of the information might have increased with the visualization and stimulated the decision confidence. Further, increased risk perception was explained by visualization being a catalyst for understanding and imagining a risky situation in an easier fashion. Despite the fact that participants were expected to make less risky decisions when the model was presented, their risk taking behavior was increased. We linked the reason of this outcome to the improved decision confidence, which might have encouraged the risk taking behavior of the respondents.

As a result, visualization of security leaves many open questions. With null results on the hypothesized main effects, our data rather supports the view that rich visuals are not necessarily useful for decision making in the security domain. It may even be the case that ad hoc visualizations turn out to be useless or even counter-productive, if they increase confidence in wrong decisions, as observed in our small sample of educated professionals. To prevent such undesirable outcomes, future development of visualization approaches and graphical modeling languages should be accompanied by user studies. For a broader outlook, as many security decisions affect others (e.g. stakeholders), more emphasis should be put on how the visualization facilitates the understanding of which parties are at risk and who is responsible for managing it.

ACKNOWLEDGEMENTS

The authors are grateful to all volunteers who participated in the survey. They also thank Dominique Machuletz for excellent feedback and Elissa Redmiles for very supportive shepherding.

REFERENCES

[1] Eppler, M. J., & Aeschimann, M. (2009). A systematic framework for risk visualization in risk management and communication. *Risk Management, 11*(2), 67–89.

[2] Horwitz, R. (2004). Hedge Fund Risk Fundamentals: Solving the Risk Management and Transparency Challenge. *Bloomberg Press*, p.83.

[3] Gates, C., & Engle, S. (Eds.). (2013). Reflecting on visualization for cyber security. *Intelligence and Security Informatics*, (ISI) 275–277.

[4] Hall, P., Heath, C., Coles-Kemp, L., Tanner, A. (2015). Examining the contribution of critical visualisation to information security. *In: Proceedings of the 2015 New Security Paradigms Workshop*. ACM

[5] Labunets, K., Massacci, F., & Paci, F. (2017, February). On the equivalence between graphical and tabular representations for security risk assessment. *In International Working Conference on Requirements Engineering: Foundation for Software Quality* (pp. 191-208). Springer, Cham.

[6] Li, E., Barendse, J., Brodbeck, F., Tanner, A. (2016). From A to Z: developing a visual vocabulary for information security threat visualisation. *In: Graphical Models for Security*

[7] Mayer, R. E. (2001). Multimedia Learning: *Cambridge University Press*.p.1

[8] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93–114.

[9] Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research, 1*(3), 153–161.

[10] Rogers, R. W., Cacioppo, J. T., & Petty, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychophysiology: A sourcebook* (pp. 153–177).

[11] Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health psychology*, 12(4), 324.

[12] Becker, M. H. (1974). The health belief model and personal health behavior. *Health Education Monographs, 2*, 324–508.

[13] Harrison, J. A., Mullen, P. D., & Green, L. W. (1992). A meta-analysis of studies of the health belief model with adults. *Health Education Research, 7*(1), 107–116.

[14] Garrett Chris (2004). Developing a Security-Awareness Culture – Improving Security, *from SANS Institute*

[15] Beresnevichiene Y., Pym D.and Shiu S. (2010). Decision support for systems security investment, *IEEE/IFIP Network Operations and Management Symposium Workshops*, pp. 118-125.

[16] Baldwin, A., Beres, Y., Duggan, G.B., Mont, M.C., Johnson, H., Middup, C., Shiu, S (2013). Economic Methods and Decision Making by Security Professionals. *In: Schneier B. (eds) Economics of Information Security and Privacy III*

[17] Ponemon Institute (2013). The State of Risk-Based Security. Retrieved April 02, 2015, from *http://www.tripwire.com/ponemon/2013/#collaboration*.

[18] Peter Sarlin (2014). Macroprudential oversight, risk communication and visualization, Goethe University Frankfurt, RiskLab Finland.p.2

[19] Bettman, J. R., & Kakkar, P. (1977). Effects of information presentation format on consumer information acquisition strategies. *Journal of Consumer Research*, 233–240.

[20] Lurie, N. H., & Mason Charlotte (2007). Visual Representation: Implications for Decision Making. *Journal of Marketing*, *71*(1), 160–177.

[21] Fink, G. A., North, C. L., Endert, A., & Rose, S. (Eds.). (2009). *Visualizing cyber security: Usable workspaces:* IEEE.

[22] Chi, S.-D., Park, J. S., Jung, K.-C., & Lee, J.-S. (Eds.). 2001. *Network Security Modeling and Cyber Attack Simulation Methodology. : Vol. 2119*.

[23] Schweitzer, D., Quist, D., & Goodall, J. R. (2012). VizSec 2012: Proceedings of the ninth International Symposium on Visualization for Cyber Security: Seattle, Washington, USA, October 15, 2012. *ACM international conference proceedings series.* New York, New York: Association for Computing Machinery.

[24] W.K. Brotby (2009): Information security management metrics: a definitive guide to effective security monitoring and measurement. CRC Press.

[25] Sommestad, T., Ekstedt, M., & Johnson, P. (2010). A probabilistic relational model for security risk analysis. *Computers & Security*, *29*(6), 659–679.

[26] P Bresciani, A Perini, P Giorgini, F Giunchiglia, J Mylopoulos (2004). Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3), 203–236.

[27] Jan Jürjens (Ed.). (2002). Using UMLsec and goal trees for secure systems development.

[28] Alexander, I. (Ed.). (2002). Initial industrial experience of misuse cases in trade-off analysis: *IEEE*.

[29] Band, I., Engelsman, W., Feltus, C., González, S. P., Hietala, J., Jonkers, H., & Massart, S. (2015). Modeling Enterprise Risk Management and Security with the Archimate Language*:* The Open Group. Retrieved May 10, 2015, from https://pure.fundp.ac.be/ws/files/12344751/Modeling_Enterprise_Risk_Management_and_Security_with_the_ArchiMate_Language.pdf.

[30] Card, S. K., Mackinlay, J. D., & Shneiderman, B. (1999). Readings in Information Visualization: Using Vision to Think*: Morgan Kaufmann Publishers*.

[31] Chen, C. (2006). Information Visualization: Beyond the Horizon: *Springer*.

[32] Tegarden, D. P. (2000). Business Information Visualization. *Communications of AIS*, *1*. Retrieved April 30, 2015.

[33] DeSanctis, G. (1984). Computer Graphics as Decision Aids: Directions for Research. *Decision Sciences*, *15*(4), 463–487.

[34] Vessey, I. (1991). Cognitive Fit: A Theory-Based Analysis of the Graphs Versus Tables Literature*. *Decision Sciences*, *22*(2), 219–240.

[35] Wang, Y., Wang, Y., Patel, S., & Patel, D. (2006). A layered reference model of the brain (LRMB). *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, *36*(2), 124–133.

[36] Wang, Y., Dong Liu, & Ruhe, G. (Eds.). 2004. Formal description of the cognitive process of decision making. Cognitive Informatics, 2004. *Proceedings of the Third IEEE International Conference*

[37] Sniezek, J. A. (1992). Groups under uncertainty: An examination of confidence in group decision making. *Organizational Behavior and Human Decision Processes*, *52*(1), 124–155.

[38] Bingi, R. P. (1995). The effect of decision aids on decision confidence and decision success: an empirical investigation, Texas Tech University.

[39] Kasper, G. M. (1996). A theory of decision support system design for user calibration. *Information Systems Research*, *7*(2), 215–232.

[40] Koriat, A., Lichtenstein, S., & Fischhoff, B. (1980). Reasons for confidence. *Journal of Experimental Psychology: Human learning and memory*, *6*(2), 107.

[41] Schwenk, C. H. (1986). Information, cognitive biases, and commitment to a course of action. *Academy of Management Review*, *11*(2), 298–310.

[42] Robinson, M. D., Johnson, J. T., & Robertson, D. A. (2000). Process versus content in eyewitness metamemory monitoring. *Journal of Experimental Psychology: Applied*, *6*(3), 207

[43] Phillips, B., Prybutok, V. R., & Peak, D. A. (2014). Decision Confidence, Information Usefulness, and Information Seeking Intention in the Presence of Disconfirming Information. *Informing Science: the International Journal of an Emerging Transdiscipline*, *17*.

[44] Stone, E. R., Yates, J. F., & Parker, A. M. (1994). Risk communication: Absolute versus relative expressions of low-probability risks. *Organizational Behavior and Human Decision Processes*, *60*(3), 387–408.

[45] Lipkus, I. M., & Hollands, J. G. (1999). The visual communication of risk. *JNCI monographs*, *1999*(25), 149–163.

[46] Mayer, R. E. (1989). Systematic thinking fostered by illustrations in scientific text. *Journal of Educational Psychology*, *81*(2), 240.

[47] Mayer, R. E. (1996). Learning strategies for making sense out of expository text: The SOI model for guiding three cognitive processes in knowledge construction. *Educational psychology review*, *8*(4), 357–371.

[48] Paivio, A. (1986). *Mental Representations: A Dual Coding Approach:* Oxford University Press.

[49] Chandler, P., & Sweller, J. (1991). Cognitive load theory and the format of instruction. *Cognition and instruction*, *8*(4), 293–332.

[50] Sweller, J. (1999). *Instructional Design in Technical Areas.* Camberwell, Victoria, Australia: Australian Council for Educational Research.

[51] Wittrock, M. C. (1989). Generative processes of comprehension. *Educational psychologist*, *24*(4), 345–376.

[52] Mayer, R. E., & Gallini, J. K. (1990). When is an illustration worth ten thousand words? *Journal of Educational Psychology*, *82*(4), 715.

[53] Mayer, R. E., & Moreno, R. (1998). A split-attention effect in multimedia learning: Evidence for dual processing systems in working memory. *Journal of Educational Psychology*, *90*(2), 312.

[54] Mayer, R. E., & Gallini, J. K. (1990). When is an illustration worth ten thousand words? *Journal of Educational Psychology*, *82*(4), 715.

[55] Mayer, R. E., & Sims, V. K. (1994). For whom is a picture worth a thousand words? Extensions of a dual-coding theory of multimedia learning. *Journal of Educational Psychology*, *86*(3), 389.

[56] Masri, K., & Gemino, A. (2006). *What Are You Staring At? Comparing Iconic Graphics With Text In Entity Relationship Diagramming. ASAC.* Retrieved May 01, 2015, from .

[57] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, *34*(3), 549–566.

[58] European Commission (Ed.) (2013). Eurobarometer 79.4, *Data file Version 3.0.1*. Brussels: GESIS Data Archive, Cologne.

[59] Vessey, I. (1991). Cognitive Fit: A Theory-Based Analysis of the Graphs Versus Tables Literature*. *Decision Sciences*, *22*(2), 219–240.

[60] O'Reilly, C. A. (1980). Individuals and information overload in organizations: Is more necessarily better? *Academy of Management Journal*, *23*(4), 684–696.

[61] Phillips, B., Prybutok, V. R., & Peak, D. A. (2014). Decision Confidence, Information Usefulness, and Information Seeking Intention in the Presence of Disconfirming Information. *Informing Science: the International Journal of an Emerging Transdiscipline*, *17*.

[62] S. Egelman, L. F. Cranor, and J. Hong (2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings: *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference*, 1065–1074.

[63] Weinstein, N. D. (1984). Why it won't happen to me: perceptions of risk factors and susceptibility. *Health psychology*, *3*(5), 431.

[64] Weinstein, N. D. (1987). Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of behavioral medicine*, *10*(5), 481–500.

[65] Gerrard, M., Gibbons, F. X., & Reis-Bergan, M. (1999). The effect of risk communication on risk perceptions: the significance of individual differences. *JNCI monographs*, *1999*(25), p.98.

[66] Lichtenstein, S., & Fischhoff, B. (1977). Do those who know more also know more about how much they know? *Organizational Behavior and Human Performance*, *20*(2), 159–183.

[67] Simon, M., & Houghton, S. M. (2003). The relationship between overconfidence and the introduction of risky products: Evidence from a field study. *Academy of Management Journal*, *46*(2), 139–149.

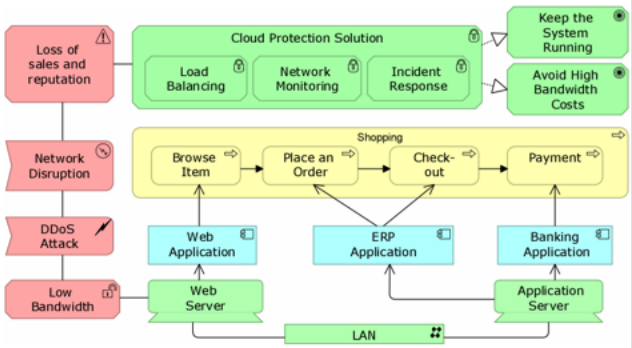
Appendix

A.1 Questionnaire material

Figure A.1: Tested security case with the graphical model

Core business processes:

The main shopping process is based on typical e-commerce purchasing steps (search - order - check out - payment). Firstly, by using the web portal the customer browses and searches for an item. Upon finding the item, (s)he places order and proceeds to the check-out process. In the payment process, payment data is captured and sent to the payment gateway.



Technical architecture:

* The web server supports the web application which facilitates the front-end of the item browsing process. It is connected to the application server via LAN (Local Area Network).
* The application server supports the ERP (Enterprise Resource Planning) application for ordering and check-out processes as well as the banking application for the payment process.

Result of the system vulnerability assessment:

It is found that the network bandwidth of the online store is rather low to defend the system against possible DDoS attacks. In case of a DDoS attack, low bandwidth can cause web server to not be able to respond to customer requests which means loss of sales and reputation for the Natursale. In order to keep the system running and avoid high bandwidth costs, we suggest mitigating the risk by a cloud DDoS protection solution. Professional security companies offer DDoS solution packages over the cloud where they can quickly balance the bandwidth and monitor the state of the network as well as offer 24/7 incident response.

A.2 Survey questions with relation to hypotheses

Table A.1: Relevant survey questions

Hypothesis	Measurement	Question	Relation to theory
H1	Number of correct comprehension questions answered	• What is the vulnerability of the current system against DDoS attacks? • Which of the choices below does not fit to the goal of the suggested cloud protection solution? • Why does the consulting company suggest a cloud protection solution? • What is the impact of possible a DDoS attack to the business of Natursale? • Which business process is directly affected by the DDoS attack?	Based on multimedia principle of CTML
$H_{2.1}$	Participants are asked to rank their IT security background	• Please indicate your level of Information Security related knowledge?	Based on individual differences principle of CTML
$H_{2.2}$	Three spatial ability measurement questions are asked	• Which of the five groups can be combined to make the figure below? • Which is the mirror image of the figure below? • An A4 paper is folded as shown and a hole is made where marked by a dot. When unfolded, where on the paper will the holes show up?	Based on individual differences principle of CTML

H3	Questions asked to reveal the decision confidence after the investment decision is made	• Overall, I am very confident regarding the optimality of my product choice decision • Overall, I would recommend my product choice to others • I think my product choice is hard to defend	Ad hoc assumption
H4	Risk perception questions are asked according to PMT theory	• Potential harm of a DDoS attack on Natursale's business would be serious • It is very likely that Natursale will become a victim of DDoS attacks in the next 12 months • Potential impact of DDoS attack on Natursale's item browsing process would not be serious • It is very likely that attackers will target the larger organizations rather than Natursale • It is very likely that a potential DDoS attack will cause a significant outage that will result in financial losses to Natursale	Ad hoc assumption
H5	Two financial risk aversion questions are asked to reveal if the participant is tending to choose the safer choice	It is estimated that Natursale potentially might suffer 2 DDoS attacks per year. The evaluation shows that two of the attacks, in total, can cost approximately 800.000 $ in loss of sales, reputation and productivity. (Yearly revenue of Natursale is considered around $100 million.) • Which solution from Security Company A and B would you choose to mitigate the DDoS attack?	Ad hoc assumption

A.3 Descriptive statistics

A.3.1 Risk perception descriptive statistics

The intraclass correlation (ICC) was used to evaluate the reliability of the risk perception questions. The correlations of mirror questions which are risk consequence mirror question (CMQ) and risk likelihood mirror question (LMQ) as well as risk consequence (CQ), risk likelihood (LQ) and their combination (CLQ) are displayed below.

Table A.2: Risk perception correlation matrix and descriptive statistics (mirror questions included)

Question	CQ	CMQ	LQ	LMQ	CLQ	M	N	S.D.
CQ						4.07	85	.704
LQ	.238					3.07	85	.753
CMQ	.195	.135				3.89	85	1.01
LMQ	.043	.441	-.113			2.76	85	.947
CLQ	.586	.267	.260	.135		4.08	85	.621
α = .527								

A.3.2 Decision confidence descriptive statistics

The intraclass correlation (ICC) was used to evaluate the reliability of the decision confidence questions as well. Table below summarizes reliability ratings and descriptive statistics of the decision confidence questions.

Table A.3: Reliability of the decision confidence questions with descriptive statistics

Question	Q1	Q2	Q3	M	N	SD
Q1				3.64	85	.93
Q2	.78			3.65	85	.83
Q3	.42	.32		3.31	85	1.12
α = .73						