INDIVIDUAL PREFERENCES IN SECURITY RISK DECISION MAKING: AN EXPLORATORY STUDY UNDER SECURITY PROFESSIONALS

JOHAN J. DE WIT[1], WOLTER PIETERS[2] & PIETER H. A. J. M. VAN GELDER[1]
[1]Delft Technical University, The Netherlands
[2]Radboud University, The Netherlands

ABSTRACT

Risk assessments in the (cyber) security domain are often, if not always, based on subjective expert judgement. For the first time, to the best of our knowledge, the individual preferences of professionals from the security domain are studied. In on online survey they are asked to mention, rate and rank their preferences when assessing a security risk. The survey setup allows to differentiate between easily accessible or "on top of mind" attributes and guided or stimulated attributes. The security professionals are also challenged to both non-compensatory and compensatory decision making on the relevance of the attributes. The results of this explorative study indicate a clear difference and shift in the individual perceived relevance of attributes in these different settings. Another remarkable finding of this study is the predominant focus on impact attributes by the respondents and the less significant position of likelihood or probability. The majority of professionals seem to ignore likelihood in their security risk assessment. This might be due to so called probability neglect as introduced by other scholars. the security in organisations and society is depending on the assessment and judgement of these professionals, understanding their preferences and the influence of cognitive biases is paramount. This study contributes to this body of knowledge and might raise attention to this important topic in both the academic and professional security domain.

Keywords: security risk assessment, decision making, risk management, decision biases, preferences, probability neglect.

1 INTRODUCTION

The security risk field is dealing with malicious, and therefore manmade, risks. Risks in general contain a level of uncertainty by nature as they involve a future state of affairs. The aspect of malicious intent of security risks add an extra dimension to this uncertainty. Malicious actions, like for example an intrusion, usually are meant to be unpredictable, concealed and evade existing risk controls.

The dynamic context of security risks, with ever changing modus operandi, in combination with the large variety of situations, both in location and time, add to the uncertainty. Because of this information about past security risks and events, if available, is often not sufficient to estimate or predict future security risk. The assessment of the uncertainty of security risks, therefore, is for a large part based on expert judgement rather than based on evidence or objective data.

The individuals assessing security risks, in this study referred to as security professionals, often, if not always, apply a risk management process of some sort to structure their assessment. The various risk management processes contain obvious process stages like: establishing the context, risk identification, risk analysis, risk evaluation and risk treatment.

So far little scientific studies are conducted exploring individual preferences and priorities guiding security professionals in their daily praxis of security risk decision making during these risk management processes. These professionals play a decisive or advisory role in security risk treatment, hence, they are determining or at least influencing the security in organisations and society. Understanding their individual preferences and priorities is of vital

WIT Transactions on The Built Environment, Vol 206, © 2021 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE210161

importance to understand their security risk judgement. The purpose of this exploratory study is to examine the criteria, further referred to as attributes, and their priority, security professionals consider when assessing a security risk.

An online survey is conducted under security professionals of both the physical and cybersecurity domain. The survey set up is explained in more detail in the Method and Materials section.

This study is, for the first time, exploring security risk assessments by security professionals. What are the individual preferences and priorities of security professionals? Do they change after a "second thought"? Is individual expertise influencing these preferences? The purpose of this exploratory study is to enhance our understanding of individual decision making influencing the security in our society.

Section 2 presents a brief overview of the theoretical background of security risks, risk assessments and decision making. In Section 3 the research method is explained followed by the Results and Analysis section. This paper ends with conclusions and discussion in Section 5.

2 SECURITY RISK ASSESSMENTS AND DECISION MAKING

In this section first the characteristics of security, security risks and risk management processes are described followed by a theoretical background of decision making, cognitive biases, especially the availability heuristic.

2.1 Security, security risks and risk management

Keeping objects and organisations secure is the prime task of security professionals [1]. They have a decisive or advisory role in dealing with security risks. According to the ISO 31000, Risk management – Principles and guidelines, risk is "the effect of uncertainty on objectives". According to Hansson [2] "knowledge about a risk is knowledge about the unknown". This knowledge is in many cases incomplete and, therefore, will have to be supplemented or even replaced by expert judgment [3]. The latter is certainly the case in security related events.

Expert judgement is considered a degree of belief, based on tacit knowledge and expertise [4]. These subjective interpretations and assessments are not only based on "hard-to-measure" expertise but are also prone to numerous cognitive biases and heuristics. This has led many scholars to question the viability of such uncertainty assessments. Still in many domains, like security, there are no alternatives or objective procedures available. Therefore, intuitive judgements of uncertainty play an essential role in decisions [5].

2.2 Decision making

"A decision is a commitment to a course of action that is intended to produce a satisfying state of affairs" [6]. A decision involves a range of options for possible action or inaction. Decision options are further referred to as alternatives in this study. The decision agent is supposed to be equipped with a set of preferences based on objectives or goals.

In order to reach a final judgement and be able to select a possible decision alternative, the agent needs to analyse and differentiate the available alternatives [7]. Each alternative is, therefore, defined by a set of attributes associated with consequences when materializing. An attribute is defined as a certain aspect of an alternative. It is used to measure performance in relation to an objective.

Besides this more functional explanation of decision making, focussed on maximizing subjective expected utility, other functionalist metaphors, like accountability, influence human decision making. “Accountability refers to the implicit or explicit expectation that one may be called on to justify one’s beliefs, feelings and actions to others” [8]. Due to the responsibility for managing something as important as security risks, the security professionals in this study can be expected to, consciously or unconsciously, consider accountability in their decisions.

The individual response to attributes consists of two main components: an affective response and a cognitive response. These relate to the so-called dual-process models. The most renown of these models is the system 1 and 2 model by Kahneman [9]. The affective response is related to system 1 which is considered to be more intuitive, automatic, fast, experience based and requires little cognitive effort. System 2, on the other hand, is considered deliberate, slow, concentrated, compensatory, and demands considerable cognitive effort. In the huge body of work on decision making that has evolved since the 1970s multiple heuristics and biases are identified and analysed. These heuristics and biases influence or even direct individual decision making.

This study focusses on availability (heuristic) which is considered one of the prominent general-purpose heuristics. A large body of research demonstrated that judgements in general are based on the information that is most accessible to the decision agent at the time of the judgement. Both ease of recall and content of recall (the number of associations) influences the estimation of likelihood and thus perceived risk.

Van der Pligt and Vliek [10] added a valuable observation to the availability heuristic. Combining the ease of recall and content of recall to decision attributes not only influences the estimation of possible frequencies, but also influences the judgement of prevalence or commonness of a situation. A prevalent situation or attribute is widely accepted or favoured and this leads these scholars to the observation that prevalence adds to the weight of an attribute. In other words: availability of information of an attribute leads to a higher priority of this attribute.

3 METHOD AND MATERIALS

This survey is committed to explore the attributes of security risks security professionals consider and prioritize when assessing security risks. The attributes of security risks which are considered by security professionals during their security risk assessment are, therefore, collected and analysed. The explorative results are retrieved via an online survey conducted between June 13, 2019 and August 28, 2019. Participation in the survey was promoted in both the IT and physical security professional community. It was promoted via LinkedIn and Twitter, both in general and in special interest groups like Security management, ASIS Europe and ASIS International, Dutch cybersecurity platform. Second, a direct email campaign was launched targeting the existing professional network of the researchers. Third, the survey was published via the website of The Hague Security Delta, a Dutch security cluster of businesses, governments and knowledge institutions. Finally, the survey was promoted on several conferences and meetings via flyers. The sample of respondents (N = 248) is regarded to be a convenience sample.

To challenge the respondents the survey starts with an open ended question. This question asks them to come up with the attributes (in the survey referred to as criteria) they consider when assessing security risks. These answers express what is “on top of mind” and quickly available for the respondents in a blind recall without prompting from external stimuli. This open ended question allows the respondents to answer based on their complete knowledge, perception and experience without restrictions. The question offers a maximum of 10 answer

options (first field forced response). This question evokes the respondents to show their attitude based on the attributes they take into account when judging security risks and measures. The answers to these questions serve as an index of quickly or most available attributes. This availability of attributes is related to the well-known availability heuristic. The answers to these open ended questions reflect the priority of, in this case, attributes related to security risk assessment. They can be considered as most prominent by the security professionals at the point of time of answering the survey.

To be able to determine the priority of attributes in multiple attribute decision making in a fuzzy environment two subsequent processes are involved: rating and ranking of attributes [11]. In the second part of the survey the respondents are asked to assign a priority to a predefined list of 28 security risk attributes (see Table 1). Each of the presented attributes can be rated using a five point Likert scale: extremely important, very important, moderately important, slightly important, not at all important. As the rating is done per individual attribute the rating is non-compensatory. The predefined list of attributes is derived from risk assessment tools like the ISO 27005, Information security risk management and the ASIS International Risk assessment and the SCM model. Four attributes influencing risk perception are also added to the list dread (fear), knowledge of the risk, whether or not the exposure to a risk can be influenced and finally if the risk can be managed or controlled.

Table 1: Predefined security risk attributes.

Predefined security risk criteria:	
Context impact criteria:	**Individual/personal impact criteria:**
1. Perceived impact (general)	17. Personal responsibility/ accountability
2. Impact on health and safety of employees	18. Damage to personal reputation
3. Impact on health and safety of customers, or visitors	19. Management attention
4. Impact on surroundings/community	20. Personal liability
5. Impact on business process (including IT downtime)	21. Personal financial loss
6. Impact on supply chain	22. Personal conscience
7. Financial impact	23. Regret of no or inadequate action
8. Legal impact/liability	**Likelihood/probability:**
9. Environmental impact	24. Probability/likelihood of risk (general)
10. Damage to the reputation of the organization	**Other/risk perception:**
11. Impact on public opinion	25. Fear of a security risk
12. Physical damage to assets	26. Involuntariness of risk taking
13. Data loss	27. Uncontrollability of risk
14. Data disclosure (including privacy sensitive data)	28. Lack of knowledge about a risk
15. Loss of data integrity	
16. Disclosure or loss of intellectual property	

In the third part of the survey the respondents are forced to set priorities over the 28 predefined attributes. They are asked to rank their top 10 (1 is the most important attribute, etc.). To avoid order biases, or response order bias the list of predefined attributes is

automatically randomized for each participant. At this point in the survey the respondents are asked to rethink their position on risk attributes for the third time and this time they even need to apply compensatory mental models. This is considered to be system 2 thinking. Comparing the answers to the open ended questions of the first part and the ranking answers to this third part is considered to show the difference in the judgement of security risk attributes between system 1 and system 2.

The survey ends with nine questions on individual characteristics: functional description, number of years in current position, number of years security expertise, number of years professional expertise, age, education level, specific security trainings, job sector, size of organization in number of employees.

Open ended questions usually lower the completion rate of a survey due to the required cognitive effort of the respondents. Taking survey fatigue into account the order of the survey questions is organized to start with the most demanding open-ended questions and lower the cognitive effort with each question. After agreeing the consent statement (N=248) 60% of the respondents stopped the survey at the start of the open ended questions. Of the remaining 99 participants 81 completed the entire survey.

4 RESULTS AND ANALYSIS

In this section the results of the survey are discussed in three parts: the result and analysis of the open ended questions, the results and analysis of the rating questions, the results and analysis of the ranking questions. Finally these results are combined and compared.

4.1 Part one: Open ended questions

The open ended question is answered in plain text by 99 respondents. Four of these did not answer seriously, their answers are excluded from the analysis. To answer the first question: “When you assess a security risk, which criteria do you consider or take into account during your assessment?”, in total 463 free text fields are filled, containing 516 identifiable and interpretable answers. These answers are considered to be “on top of mind”, easily available and primarily originating from system 1 thinking.

For a first interpretation of the answers the method of manual inductive or grounded coding is applied, the coding process thus allowed the main attributes and their structure to emerge. The coding frame that emerged from the manual inductive coding process revealed common risk components beyond the two expected general risk components following the narrow definition of risk: probability/likelihood and consequence/impact. The respondents seem to have included components of the risk management process leading to the final assessment of security risks. In the narrow scope as intended by the researchers risk assessment is forming a judgment of a security risk based on the two general attributes likelihood and consequence.

The observed categories are in line with the risk management process as detailed in security risk standards like the American National Standard: Risk Assessment, issued by ANSI, ASIS and RIMS [13], see Fig. 1.

As impact and consequence are not specifically defined in the survey the vast majority of the respondents used “impact”, only four used the word “consequence”. In the analysis of the answers in this study the categories impact an consequence are combined. This study focusses on the narrow definition of risk assessment (see Fig. 1).

The categories emerging from the inductive coding process fit the predefined risk attributes as presented in Section 3. The list of predefined risk attributes, however, contains

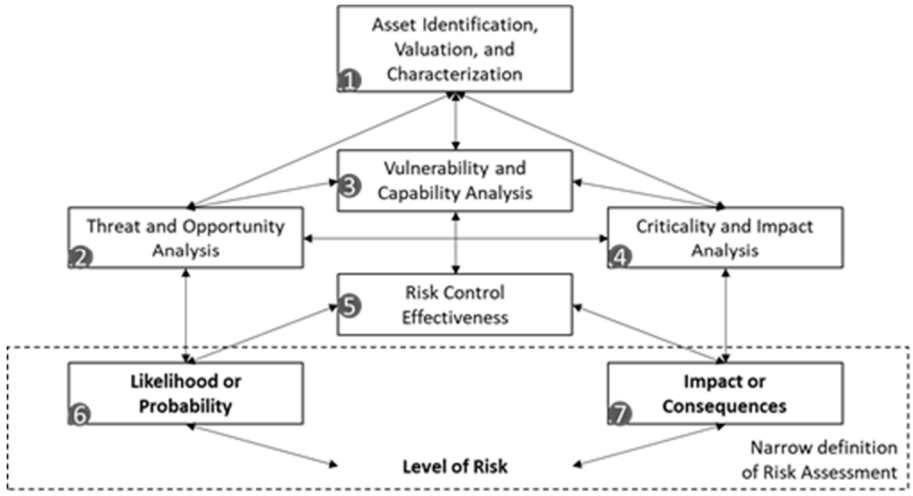

Figure 1: "Determining the level of risk", risk management process according to American National Standards Institute.

attributes that seem to be "not on top of mind" and they are not mentioned by the respondents. These attributes mainly concern individual/personal impact attributes and risk perception attributes. There are also three impact categories that some of the respondents pointed out that were not included in the predefined criteria list: Impact on trust, impact on/for customers, and political/national impact. The results of the open ended answers limited to the intended narrow definition of risk assessment are presented in Table 2.

A reliability analysis was carried out on the answers to the open ended questions. Cronbach's alpha showed the answers to reach low internal reliability, $\alpha = 0.469$.

Further correlation analysis showed various significant but low correlations between the individual attributes (r values between 0.21 and 0.492). The correlation between attribute 14 and 15 reached a moderate level ($r = 0.688$, $p < 0.05$). The inductive coding process shows clearly that the largest answer category relates to impact (192 answers). The vast majority of respondents, 87%, mentions one or more impact attributes.

It is remarkable to observe that only 43% of the respondents mentions the other main component of risk expressing uncertainty. Likelihood, probability, frequency or chance is mentioned only by 42 respondents. As almost all respondents mention impact criteria and less than half of them mentions likelihood there seems to be a predominant focus on impact/consequences.

Using the chi-squared tests there are no significant influences of individual characteristics observed. Education level, specific security trainings, age, and professional an security experience do not seem to influence the answers to the open ended questions.

4.2 Part two: Rating criteria

In the second part of this study the predefined list of risk attributes is presented to the respondents. Each of the presented attributes can be independently rated using a five point Likert scale: extremely important, very important, moderately important, slightly important,

Table 2: Descriptive analysis, inductive coding, sub categories of answers within the categories impact/consequence and likelihood/probability.

Question 1: When you **assess a security risk**, which criteria do you consider or take into account during your assessment?			
Free text entries, manually, inductive or grounded coding		Number of answers:	Percentage of respondents:
1	Perceived impact of the security risk	50	53%
2	Impact on health and safety of employees	23	24%
3	Impact on health and safety of customers, visitors	–	–
4	Impact on surroundings/community	10	10%
5	Impact on business process (including IT process/ downtime)	27	28%
6	Impact on supply chain	7	7%
7	Financial impact	13	14%
8	Legal impact/liability	3	3%
9	Environmental impact	4	4%
10	Damage to the reputation of the organisation	14	15%
11	Impact on public opinion	–	–
12	Physical damage to assets	8	8%
13	Data loss	11	11%
14	Data disclosure (including privacy sensitive data)	9	9%
15	Loss of data integrity	4	4%
16	Disclosure or loss of intellectual property	2	2%
17	Personal responsibility/accountability	2	2%
18	Damage to personal reputation	–	–
19	Management attention	2	2%
20	Personal liability	–	–
21	Personal financial loss (e.g. dismissal, loss of incentives)	–	–
22	Personal conscience	–	–
23	Regret of no or inadequate action	–	–
24	Probability/likelihood of risk	42	43%
25	Fear of a security risk	–	–
26	Involuntariness of risk taking	–	–
27	Uncontrollability of risk	–	–
28	Lack of knowledge about a risk	–	–
	Impact on trust	2	2%
	Impact on/for customers	5	5%
	Political/national impact	3	3%

not at all important. This list of attributes is considered an external stimulus to the respondents. It is analysed how this stimulus influences the priorities of the respondents.

The results show the influence of a stimulus: the respondents rate the majority of the attributes important even if they did not have them on top of mind at the first question. On average (the red graph in Fig. 2) the rating concentrates in the vicinity of “very important”.

The reliability analysis (Cronbach's alpha) showed the rating to reach high internal reliability, $\alpha = 0.88$.

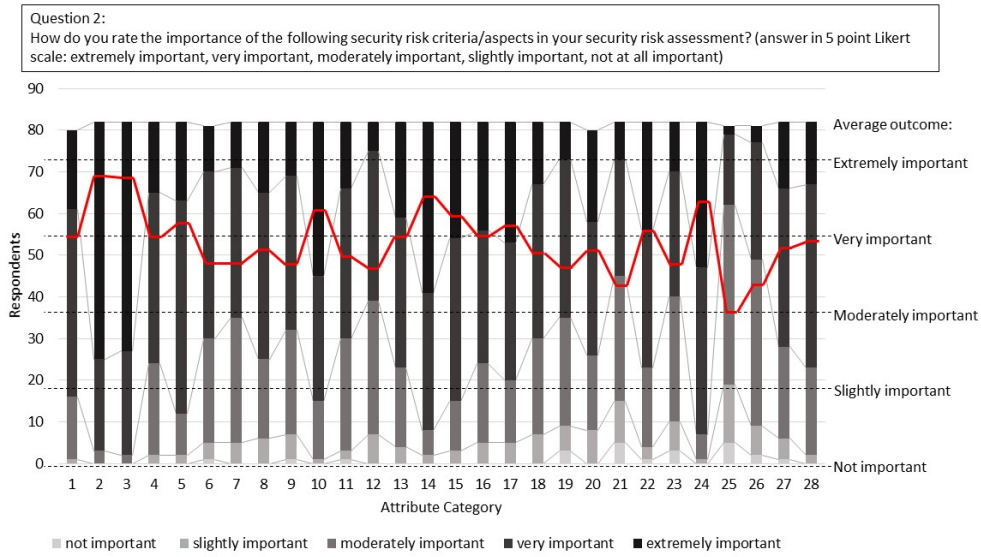

Figure 2: Descriptive analysis, rating of predefined risk attributes.

The absolute results of these answers are not considered of much value because the rating is assigned non-compensatory. The relative differences between the answers are considered of more value to be able to identify individual preferences.

The average answer is calculated by assigning a value to the Likert scale (extremely important is 5 points, etc.). The Likert scale is thus considered a continuous variable.

Correlation analysis showed various significant but low to medium correlations between the individual attributes (r values between 0.212 and 0.640). The only strong and significant correlation is identified between attribute 2 and 3 ($r = 0.900$, $p < 0.05$).

4.3 Part three: Ranking the attributes

When rating the attributes as analysed in the previous section respondents do not have to compare the attributes and can express their preferences without the need to make trade-offs. In the third part of the survey, however, the respondents are asked to rank the attributes and compose their individual top 10 of most important attributes. This is a form of compensatory decision making in which the aspects of and preferences to an attribute need to be weighed. This kind of decision making takes considerable cognitive effort and is considered a system 2 process. Each respondent can freely assign a rank (1 is most important etc.) to the 28 predefined attributes. To avoid order bias the attributes are presented in a random order to each respondent. 70 respondents completed this ranking task correctly. For overall comparison each top 10 listing is assigned a value (a number 1 listing 10 points etc.). The total value assigned to each attribute as well as the number of respondents listing an attribute in their top 10 is shown in Fig. 3.

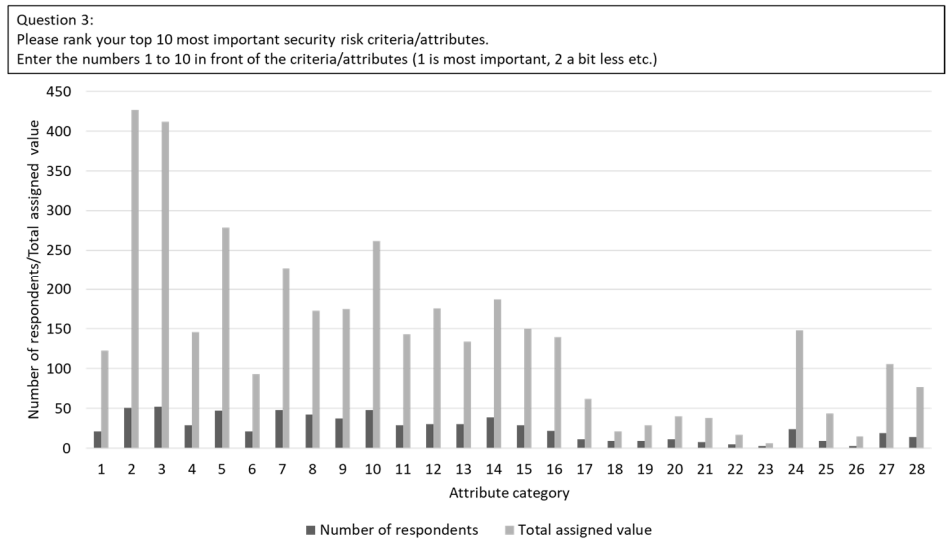

Figure 3: Descriptive analysis, ranking of predefined risk attributes.

It is clear that the impact on health and safety of employees (attribute 2) and of customers, clients and visitors (attribute 3) are overall considered the most prominent attributes in security risk assessments. This is in line with the results of the attribute rating (see previous section). Attribute 2 is listed by 73% of the respondents, attribute 3 by 74%. At the answers to the open ended questions only 24% mentioned health and safety.

The predefined list, in this experiment considered a stimulus, seem to have changed preferences of a large group of respondents.

The other main component of risk assessments: likelihood or probability shows a very different pattern. At the open ended questions 43% of the respondents state they take this attribute into account. At the rating question this attribute is rated on average between very important and extremely important. At the ranking question, however, only 34% of the respondents rank it in their top 10. This attribute received in total 148 points and rank at the 11 place of important attributes. As stated above the attribute likelihood is often listed at the open questions in combination with impact in general. These respondents (29%) seem to follow the, easily accessible, general definition of risk in their answers (risk = likelihood × impact). As they ranked the more detailed impact attributes in the third question they clearly choose impact over likelihood and might even ignore likelihood completely. These results comply to previous work, probabilities of events are not easy to define and people often disregard probability entirely [14], [15].

Table 3 finally presents an overview of the top 10 most prominent attributes over the three survey parts. The results show differences in priorities. The reaction of the respondents is clearly influenced by the list of predefined attributes that is inserted in the survey as a stimulus. A large group of respondents changes their priorities.

5 CONCLUSIONS AND DISCUSSION

The survey set up provided interesting information about the priorities of attributes in a security risk assessment. This section starts with a summary of the main results, followed by conclusions and discussion.

Table 3: Comparing the 10 most prominent attributes over three assessment processes.

	Question 1: When you **assess a security risk**, which criteria/attributes do you consider or take into account during your assessment? Please name the criterion and describe it briefly.		Question 2: How do you **rate the importance** of the following security risk criteria/attributes in your security risk assessment? (answer in 5 point Likert scale: extremely important, very important, moderately important, slightly important, not at all important)		Question 3: Please **rank your top 10** most important security risk criteria/attributes. Enter the numbers 1 to 10 in front of the criteria/attributes (1 is most important, 2 a bit less etc.)		
Top 10 rank	Top 10 is based on the proportion of the respondents listing attributes	% of resp.	Top 10 is based on the value the respondents assign to attributes (max. is 5: extremely important)	Avg. rating	Top 10 is based on the combination of the proportion of the respondents listing attributes **and** the value they assign to them (a top 1 listing is 10 points, a top 9 is 9 points etc.)	Total pts	% of resp.
1	1 Perceived impact of the security risk	53%	2 Impact on health and safety of employees	4.78	2 Impact on health and safety of employees	427	73%
2	24 Probability/likelihood of risk	43%	3 Impact on health and safety of customers, clients or visitors	4.76	3 Impact on health and safety of customers, clients or visitors	412	74%
3	5 Impact on business process (including IT downtime)	28%	14 Data disclosure (including privacy sensitive data)	4.49	5 Impact on business process (including IT downtime)	279	67%
4	2 Impact on health and safety of employees	24%	24 Probability/likelihood of risk	4.44	10 Damage to the reputation of the organisation	262	69%
5	10 Damage to the reputation of the organisation	15%	10 Damage to the reputation of the organisation	4.36	7 Financial impact	227	69%
6	7 Financial impact	14%	15 Loss of data integrity	4.23	14 Data disclosure (including privacy sensitive data)	187	56%
7	13 Data loss	11%	5 Impact on business process (including IT downtime)	4.16	12 Physical damage to assets	176	43%
8	14 Data disclosure (including privacy sensitive data)	9%	17 Personal responsibility/ accountability	4.15	9 Environmental impact	175	53%
9	12 Physical damage to assets	8%	22 Personal conscience	4.08	8 Legal impact/liability	173	60%
10	6 Impact on supply chain	7%	16 Disclosure or loss of intellectual property	4.06	15 Loss of data integrity	150	41%

WIT Transactions on The Built Environment, Vol 206, © 2021 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)

The survey started with the open ended question: "When you assess a security risk, which criteria/attributes do you consider or take into account during your assessment? Please name the criterion and describe it briefly". This question allowed the respondents to answer based on their complete knowledge, perception and experience without restrictions and without any primer or influence from the researchers. The answers to these questions serve as an index of quickly or most available attributes. These are considered as most prominent by the security professionals at the point of time of answering the survey. The results show a predominant focus on impact attributes. Both in number of answers (192) as in the proportion of respondents mentioning one or more impact attributes (87%) this attribute category seems to be considered most relevant for security risk assessments. As a risk is often defined as a combination of uncertainty or likelihood and impact it is remarkable that less than half of the respondents (43%) mentions this second risk component. This might indicate that the likelihood of a security risk is not "on top of mind" and might be considered less important.

The survey continued with a set of rating questions. The respondents are confronted with a list of 16 context impact attributes, seven individual/personal impact attributes, a likelihood/probability attribute and four risk perception attributes. They are asked to rate the importance of each attribute using a five point Likert scale. The answers show a strong internal consistency and are, on average, centred around very important. The attributes rated highest are attribute 2: Impact on health and safety of employees (average 4.78 on a scale of 5) and attribute 3: Impact on health and safety of customers, clients or visitors (average 4.76 on a scale of 5). These two attributes have reach strong correlation ($r = 0.90$, $p < 0.05$). The majority of the respondents rate these attributes extremely important (attribute 2: 69.5% of the respondents, attribute 3: 67.1% of the respondents) and very important (attribute 2: 26.8%, attribute 3: 30.4%).

The third part of the survey consisted of a ranking question: "Please rank your top 10 most important security risk criteria/attributes". In this part of the survey the respondents are forced to make trade-offs between their favourite attributes. This is considered to be compensatory decision making (system 2). As in the previous rating question the health and safety attributes (attribute 2 and 3) are considered most important by the respondents. Overall the ten most highly ranked attributes are all context impact attributes. It is remarkable that the likelihood/probability attribute is ranked in their top 10 by only 34% of the respondents and ended overall at the 11th place. These results clearly indicate a predominant focus on impact attributes in accessing security risks by security professionals. Both the personal/individual impact attributes and the risk perception attributes (based on the SCM model) are not considered of much relevance by the respondents when confronted with the compensatory ranking.

This explorative study clearly shows the influence of stimuli on decision making by security professionals. Attributes that are not "on top of mind" and might even be, consciously or unconsciously, ignored in first instance, are considered very relevant after pointing to them. The most prevalent example are the two health and safety related attributes (attribute 2 and 3). They are only mentioned by 24% of the respondents in the first part of the survey. In the second part almost all respondents rate them extremely and very important while in the third part these attributes ended at the first and second place of the overall ranking. For real life daily praxis this could mean that without guidance the respondents take different attributes into account compared to if they are helped with tooling (in this case a predefined list). The consequence of this observed behaviour is that decisions made with or without tooling could be made on different grounds and define the outcome of the decision making process. A simple checklist could already help. Based on these results it can be concluded that attributes of security decisions that are considered extremely and very

important by the majority of the respondents (see the rating question) are simply forgotten or ignored without help.

The second major finding is the lack of importance the security professionals in this study seem to appoint to likelihood/probability. At the open ended question less than half of the respondents (43%) mention likelihood or probability (87% of them mentions one or more impact attributes). At the rating, however, the majority rates it extremely important (43%) and very important (49%). When they are forced to compare the attributes in the third part of the survey only 34% of the respondents ranks likelihood/probability in their individual top 10. The assessment of likelihood or probability by people is based on their knowledge and beliefs and the assessments will thus vary over individuals. A subjective assessment of likelihood is hard for most people and they disregard likelihood entirely when confronted with risky choices [14].

Probability neglect is coined by Sunstein [15]. According to him this cognitive bias explains disregarding probability when assessing low-probability but high-impact threats. People tend to focus on the impact and ignore likelihood when strong emotions are involved. He also relates these emotions to the availability heuristic. Affect-rich decisions increase probability neglect [16]. This cognitive bias does not state that people neglect the likelihood, in situations where they can envision the impact (availability heuristic) and experience strong emotions the likelihood of occurring becomes less relevant or even irrelevant to them. Sieroń [17] added to this observation that, however the statistical likelihood of a high impact threat might be very small, people still want to avoid experiencing it. A small statistical likelihood does not mean this threat cannot affect the decisionmaker.

The respondents in this study might react according to these theories. The security risk domain is familiar to them so they can be expected to be able to envision the impact of security risks and threats. As it is there field of responsibility to decide upon or advice on managing these risks they can also be expected to feel affected by the possible impacts of these risks and threats. Finally, however small the statistical likelihood might be, the security risk or threat might materialize tomorrow and can affect their field of responsibility.

The important findings of this study might inspire other scholars to replicate them in other risk domains. They will raise awareness in both the academic as the professional security risk domain to the influence of cognitive biases on security risk decision making. This might lead to the development of de-biasing methods which can be added to existing security risk management processes enhancing security risk decision making. Managing security risks in organizations and society is of vital importance, understanding the decisions by individuals responsible for it is paramount.

REFERENCES

[1] Talbot, J. & Jakeman, M., *Security Risk Management Body of Knowledge* (Vol. 69), John Wiley & Sons, 2011.

[2] Hansson, S.O., A panorama of the philosophy of risk. *Handbook of Risk Theory*, Springer: New York, pp. 27–54, 2012.

[3] Möller, N., The concepts of risk and safety. *Handbook of Risk Theory*, Springer: New York, pp. 55–85, 2012.

[4] Cooke, R.M., *Experts in Uncertainty*, Oxford University Press: New York, 1991.

[5] Tversky, A. & Koehler, D.J., Support theory: A nonextensional representation of subjective probability. *Psychological Review*, **101**(4), p. 547, 1994.

[6] Yates, J.F., Veinott, E.S. & Patalano, A.L., Hard decisions, bad decisions: On decision quality and decision aiding. *Emerging Perspectives on Judgment and Decision Research*, Cambridge University Press, pp. 13–63, 2003.

[7] Svenson, O., Differentiation and consolidation theory of human decision making: A Frame of reference for the study of pre-and post-decision processes. *Acta Psychologica*, **80**(1–3), pp. 143–168, 1992.
[8] Tetlock, P.E., The impact of accountability on judgment and choice: Towards a social contingency model. *Advances in Experimental Social Psychology*, **25**(3), pp. 331–376, 1992.
[9] Kahneman, D., *Thinking, Fast and Slow*, Business Contact: Amsterdam, 2012.
[10] Van der Pligt, J. & Vliek, M., *The Psychology of Influence: Theory, Research and Practice*, Taylor & Francis: Abingdon, 2016.
[11] Gilovich, T., Griffin, D. & Kahneman, D., *Heuristics and Biases: The Psychology of Intuitive Judgment*, Cambridge University Press, 2002.
[12] Ribeiro, R.A., Fuzzy multiple attribute decision making: A review and new preference elicitation techniques. *Fuzzy Sets and Systems*, **78**(2), pp. 155–181, 1996.
[13] ANSI/ASIS/RIMS, *Risk Assessment RA1*, ASIS International: Alexandria, 2015.
[14] Evans, D., *Risk Intelligence: How to Live with Uncertainty*, Simon and Schuster: New York, 2015.
[15] Sunstein, C.R., Probability neglect: Emotions, worst cases, and law. *The Yale Law Journal*, **112**(1), pp. 61–107, 2002.
[16] Suter, R.S., Pachur, T. & Hertwig, R., How affect shapes risky choice: Distorted probability weighting versus probability neglect. *Journal of Behavioral Decision Making*, **29**(4), pp. 437–449, 2016.
[17] Sieroń, A., Does the COVID-19 pandemic refute probability neglect? *Journal of Risk Research*, **23**(7–8), pp. 855–861, 2020.