Seeking Risks: Towards a Quantitative Risk Perception Measure

Åsmund Ahlmann Nyre, Martin Gilje Jaatun

Seeking Risks: Towards a quantitative risk perception measure

Åsmund Ahlmann Nyre[1,2] and Martin Gilje Jaatun[2]

[1] Norwegian university of Science and Technology
Department of computer and information science
Trondheim, Norway
[2] SINTEF ICT
Trondheim, Norway
{asmund.a.nyre, martin.g.jaatun}@sintef.no

Abstract. Existing instruments for measuring risk perception have focused on an abstract version of the concept, without diving into the the details of what forms the perception of likelihood and impact. However, as information security risks become increasingly complex and difficult for users to understand, this approach may be less feasible. The average user may be able to imagine the worst case scenario should an asset be compromised by an attacker, but he has few means to determine the likelihood of this happening. In this paper we therefore propose a different approach to measuring risk perception. Based on well established concepts from formal risk analysis, we define an instrument to measure users' risk perception that combines the strengths of both traditional risk perception and formal risk analysis. By being more explicit and specific concerning possible attackers, existing security measures and vulnerabilities, users will be more able to give meaningful answers to scale items, thereby providing a better and more explanatory measure of risk perception. As part of the instrument development we also elaborate on construct definitions, construct types and the relationship between these and the corresponding risk perception instrument. Although it remains to be verified empirically, the validity of the measure is discussed by linking it to well established theory and practice.

1 Introduction

There is a fundamental relationship between risk exposure and the perceived need for protection. If there are no risks, then there is nothing that needs protection either. That is why users' intention to adopt a security measure is tied directly to the perceived risk [23]. However, when faced with

However, the problem is that perceived risk is highly subjective, and therefore varies greatly between people. There are many risk assessment methodologies, but as a rule they are quite complex, and not suitable for use by a layperson. In order to measure a layperson's risk perception, we need a simpler instrument that helps splitting the difficult question "what is the risk to your system" into manageable pieces. Even more importantly, though, the instrument should help to explain *why* the risk is perceived as it is.

A better understanding of regular users' risk perception would be an important basis for improving security technology, awareness-raising and ultimately also the uptake of security technology. This user-centric approach to risk allows security technology to focus on the risks important to the user, and thereby both gaining acceptance and motivation for its usage. The approach lends its idea from user-centric design of software systems, in that it is the users' perception that guides the design and presentation, rather than the designer's perception. This is not to say that security professionals' risk analysis should be discarded, but rather that the presentation to users should be based on their perceived risk. With a deeper understanding of the motivations behind the risk perception, it is also easier to spot misconceptions which can skew the perceived risk.

In order to gain a better understanding of risk perception, we need a model of how risk perception is formed and how it can be measured. This paper contributes a theoretical foundation and the initial step towards such a measurement instrument. To this end, we combine results from research on risk perception and well established concepts from formal risk analysis methodologies.

The remainder of this paper is organised as follows. In Section 2 we provide an overview of related work on measuring risk perception in IT. Next, in Section 3 we provide some background on previous research on judgments under uncertainty, risk perception, and risk analysis frameworks. In Section 4 we present our risk perception model and a preliminary instrument for measuring risk perception. Then we discuss the validity of our instrument in Section 5, before we give our concluding remarks in Section 6.

2 Related work

Work on risk perception has been seen when investigating the factors that affect IT technology adoption in general, and information security technology in particular. For instance Featherman and Pavlou [8, 25] showed that risk perception have a negative effect on consumers' intention to engage in online shopping. Risk perception was measured by the different facets of risks, including time risk, performance risk, financial risk and privacy risk. According to the definitions of these terms, they do not explicitly include the risks associated with active attackers. In a similar study, Kim, Ferrin and Rao [18] used the perceived privacy and security protection as well as familiarity, reputation, trust disposition and the presence of privacy seals to predict intention to adopt online shopping. The measure of privacy protection does include a scale item concerning "unautorized users (i.e. hackers)" [18], but for the most part the measure concerns the integrity and honesty of the vendor. Hörst, Kuttschreuter and Gutteling [12] and Belangr and Carter [1] both used a measure of risk perception in determining the intention to adopt e-government services. Both studies use a high level measure of perceived risk that neither caters for the different facets of risks nor active attackers.

Studies of adoption of information security technology such as anti-spyware software [4], data backup software [6] and wireless security settings [37] have used a decomposed measure of risk to predict adoption intention. That is, based on the Protection Motivation Theory (PMT) [27], these studies measure the perceived vulnerability (likelihood) and severity (impact) of an adverse event, rather than the perceived risk. The same approach is also found in research on antecedents of employees' security policy compliance [28, 11, 2]. Although the measures used are more specific on security threats and also include adversaries, they do not include perceptions of current security measures or adversaries. The foundations for risk perception in psychology is further discussed in the upcoming section.

There is an abundance of risk analysis frameworks that describe in varying degree of detail the considerations that should be taken when analysing risks. Examples of such frameworks include the OWASP Testing guide [24], OCTAVE Allegro [3], NIST RMF [36] and CORAS [20]. The focus of these frameworks is to guide corporations or security professionals in performing thorough, comprehensive and reliable risk analyses. The aim is therefore to capture a more objective assessment of security risks. For the purpose measuring subjective risk perception, these frameworks cannot be applied directly. However, they do provide valuable insights into the concept of risk and provide an important basis on which we build our risk perception instrument.

Our work differ from previous research in that it attempts to bridge the gap between risk perception measures and risk analysis methodologies. The risk perception measure we propose maintains the subjective notion of risk while being more concrete and more detailed concerning the risk concept itself. Thus we extend risk perception measures to include the common concepts of risk found in formal risk analysis methodologies.

3 Background

Since risk is all about handling uncertainties, we provide a brief introduction to the psychological process of judgement under uncertainty. The cognitive processes form a basis for understanding the existing theories of risk perception. Finally, we give an overview of the main common concepts of risk found in existing risk analysis methodologies. This is by no means intended as a complete review of either area, but rather to identify some important concepts that we use when devising a risk perception measure.

3.1 The psychology of judgment under uncertainty

There seem to be general consensus among researchers that the cognitive process may be regarded as two separate, although connected, systems [16]. One is the fast and effortless *intuition* while the other is the slow and time consuming *reason*. Epstein [7] have called these systems the *experiental system* and the *rational system*, whereas others including Kahneman and colleagues [17, 16] refer to them simply as *system 1* and *system 2*. These two systems are assumed to operate quite differently. The intuition creates the initial judgment, whereas the rational system monitors and correct obvious mistakes. Intuition is fast, automatic, effortless, emotional and capable of parallel operations, whereas the rational system is slow, effortful, conscious and controlled. Thus, intuitive judgments can be made in parallel with other tasks, without giving it much conscious thought, while rational cognition requires more attention and therefore often interrupts other cognitive tasks. That is seemingly why the intuitive system always attempts to make a suggestion, while the rational system monitors and corrects the judgments that are obviously wrong. In general Kahneman reports five ways in which a judgment is made [16]:

1. An intuitive judgment or intention is initiated, and
   (a) Endorsed by the rational system;
   (b) Adjusted (insufficiently) for other features that are recognized as relevant;
   (c) Corrected (sometimes overcorrected) for an explicitly recognized bias; or
   (d) Identified as violating a subjectively valid rule and blocked from overt expression.
2. No intuitive response comes to mind, and the judgment is computed by the rational system.

Whenever our cognition fails, it is therefore not only the failure of one system, but both. First, the intuition fails to give proper judgment, either by giving an erroneous one or by not giving one at all. Next, the rational system fails to correct the initial intuitive judgment or fails to compute a proper judgment if no initial intuitive response was created.

3.2 Rational risk perception

Fischhoff, Slovic et al. [10, 31, 35, 30] have studied antecedents or dimensions of risk perception and their influence on the perception of risk and benefit, and found that these dimensions were highly correlated. For instance, it seemed that risks that where perceived to be controllable also was perceived voluntary. Based on the correlation between dimensions, Fischoff and Slovic proposed two sets of dimensions, or factors, affecting risk perception. This has later been termed the *psychometric approach* and have been one of the key approaches to understanding risk perception. High risk is characterized by factor 1 as events which are unobservable and new, have unknown risk and delayed effect. On factor 2 high risk is characterized as events that are uncontrollable, involuntary and difficult to prevent, and have catastrophic fatal consequences involving considerable dread.

The *psychometric approach* is based to a large extent on the idea that risk perception is a conscious deliberate rational process. That being said, *dread*, being intimately associated with intuition, was found to be one of the dominant dimensions of this approach. Still, as explained by Slovic later the focus of the research was on rational cognition [32].

Critics of the approach [29] have pointed to a number of weak points, particularly the fact that factor analysis is done on average ratings of dimensions,

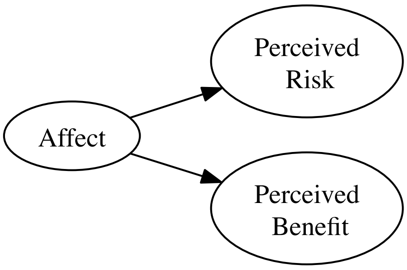

Fig. 1: The affect heuristic [33, 34]

instead of individual ratings. Although this does not necessarily mean that the factors identified in the psychometric approach are wrong, it implies that there could be many more factors than what originally was found.

3.3 Risk and affect

From the theory of decisions under uncertainty it is apparent that intuition also plays a vital part in understanding risk perception. Affect was identified as part of the *psychometric approach* (e.g. dread and fear), but has later thought to be more important in determining risk perceptions. Alhakami and Slovic (reported in [34]) found that although risk and benefit often are positively correlated in real life (i.e. great risk comes with great benefits), people's perception of risks and benefits are often negatively correlated. This discovery led them to propose that risk and benefit perceptions were guided by the affective impression of activity or technology in question. Later, this effect was termed the *affect heuristic* for risk perception [9, 33, 34]. The basic idea of this heuristic is that people record representations of prior events that are labeled according to the affective response they generate. Thus, whenever a judgment is to be made, people consult the recordings and are guided by the positive or negative affective label attached to it [9]. Positive feelings yield high perceived benefit and low perceived risk (see Fig. 1).

Finucane et al. [9] provided empirical evidence for the affect heuristic by giving different information concerning the risks and benefits of nuclear power. The study showed that whenever participants were informed of the benefits, they perceived the risks to be lower than when not receiving such information. In the same paper, the authors also used time limitations to demonstrate the affect heuristic, since system 1 operates much faster than system 2, the study suggests that under time pressure, people will rely on affect for their risk judgments.

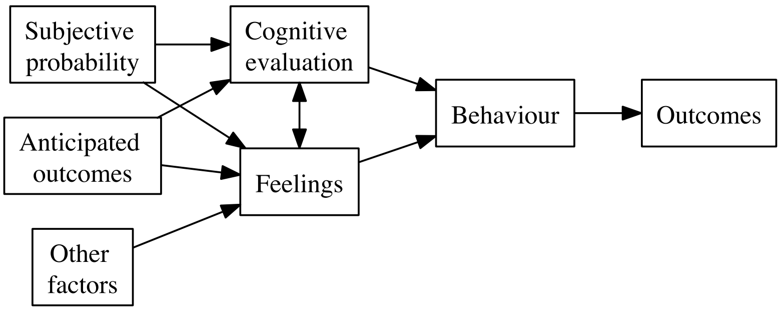

Fig. 2: Risk as feelings model [19]

Loewenstein et al. [19] propose the *"risk as feelings"*-hypothesis that feelings and cognitive evaluations are mutually influenced by each other and they both have a direct effect on behaviour, positing that emotions often produce behaviour that is in conflict with optimal behaviour. Fig. 2 illustrates these close interconnections of the two systems on risky behaviour.

3.4 Risk analysis

As mentioned in Section 2 there are several existing frameworks for conducting risk analyses. Although they are generally unsuitable to be directly transferred to a risk perception measure, the fundamental concepts on which they rely are useful. We therefore outline the predominant definitions of risk and discuss the contents of the main concepts of information security risk.

Definitions Although there are many definitions of risk in the area of information security, they all share the basic concepts of likelihood and impact. For example, ISO defines the *level of risk* as the *"magnitude of a risk, expressed in terms of the combination of consequences and their likelihood"* [13], whereas the the Open Web Application Security Project (OWASP) denotes this product of likelihood and impact as *risk*. Similarly, NIST defines risk as *"the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur"*[36]. Despite the different wording the general concept that risk concerns the combined likelihood and impact of an adverse event is generally agreed upon (see Fig. 3).

Impact The impact constitutes the negative effects an adverse event would have. The OWASP testing guide [24] distinguishes two separate kinds of impacts

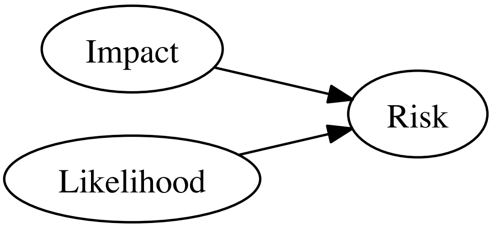

Fig. 3: The basic risk model

Table 1: Technical and business impact

Technical impact	**Business impact**
Breach of security attribute	Breach of business goals
Domain and context insensitive	Domain and context sensitive
Security knowledge	Business/domain knowledge

when determining the overall risk. Technical impact includes a breach of one or more of the security attributes such as loss of confidentiality, integrity or availability. Business impact on the other hand, is concerned with the resulting specific damage to the business or organisation. ISO-27005 [13] and NIST 800-30 [36] refer to the impact as the *business impact* and use *breach of information security (goals)* for the *technical impact*. The meaning however remains largely the same.

The technical impact is largely unaffected by the context or domain in question. Data theft will always yield loss of confidentiality (or we would not call it theft) as the technical impact, but the impact this will have on the business is very much dependent on the domain, organisation and context in which the adverse event occurred. Since the technical impact of adverse events remains relatively stable across organisations and domains it is difficult to dispute it, whereas the impact on the business may be much less obviously identified and hence often also disputed and debated. Finally, it requires security knowledge to identify the technical impact, whereas business knowledge is required to identify the corresponding business impact. Table 1 gives an overview of these differences.

There are several factors that could be investigated in order to assess the business impact. OWASP lists four such factors; financial damage, reputation damage, non-compliance and privacy violations[3]. There could potentially be many more, depending on the domain in question. In a previous study we have shown that loss of competitiveness is seen as the most important business impact of the oil and gas industry [22]. Other potential impact factors include operational discontinuity, legal liability, customer dissatisfaction or harm to personnel.

Likelihood The other main aspect of risk is the *likelihood* of an adverse event occurring. However, unlike classical safety problems there are few ways of gaining reliable statistical data to accurately calculate the probability. Metrics such as Mean Time To Failure (MTTF) are inherently difficult whenever it involves an actual non-random attacker. The problem is not only that any assessment of attack likelihood is to a great extent dependent on subjective opinions, but that it may be difficult to even have an opinion. What is the likelihood of foreign intelligence agencies conducting espionage in my company? Unless you have actually experienced it happening, it is very difficult to know what to think.

When performing risk assessments it is thus common to instead look at the factors that affect the likelihood, instead of the actual likelihood itself. The OWASP testing guide [24], ISO27005 [13] and NIST 800-30 [36] provide three sets of factors of risk likelihood:

- *Vulnerability*: Is it easy for an attacker to discover the vulnerability? If it is discovered, is it easy to exploit? Is the vulnerability common knowledge?
- *Attackers or Threat agents*: Are the potential attackers skilled to perform an attack? Do they have a motive? How often does the opportunity to exploit the vulnerability present itself? How many possible attackers are there?
- *Existing controls*: To what extent do the current security measures reduce the likelihood of exploiting the vulnerability? Is it likely that an exploit can be detected?

In the OWASP guide *existing controls* are not explicitly part of the guidance. However, implicitly it may be argued that detection mechanisms may very well be considered a control mechanism.

Some of these factors are highly inter-connected, such as how easy it is to exploit a vulnerability and how skillful the threat agents are. If the exploit is difficult, the threat agents must be very skillful in order to launch an attack; if the exploit is easy, it really does not matter how skillful the threat agents are.

4 Towards a model and measure of risk perception

Risk can be modelled in many different ways. It is common to first model a construct and next worry how to operationalize and measure it. However, as noted by Jarvis et al. [14] and Petter et al. [26], it is useful to look at these two

[3] Although the OWASP testing guide [24] does not explicitly define *financial damage*, we use it here to denote direct monetary losses as a result of an adverse event. This is to prevent confusion with *business impact*.

issues combined rather than in isolation. In this section we define the constructs of a risk perception model that is needed to create a corresponding measurement instrument. In doing so, we discuss the different types of constructs and their implications for the instrument.

4.1 Construct types

There are fundamentally three different ways in which constructs can be modelled: reflective, formative or multidimensional [14]. The way in which a construct is modelled also affects the way in which the construct can be measured. Below we present the main differences between these different types of constructs.

A *reflective* construct is used to denote a one-dimensional construct (i.e. has no sub-constructs) where the same aspect of the construct can be measured in different ways. In a standard questionnaire-type measure, this would mean that all items or questions measure the same underlying phenomenon and therefore all items are supposed to covary. Therefore, a respondent scoring low on one scale item is more likely to score low on the other scale items of the construct. Further, the scale items should be replaceable and removing one should not affect the overall measure of the construct. Reflective constructs are the predominant in Information Systems Research [26]

A much less used type of construct is the *formative* construct [26], where the measurement items are combined to *form* the construct. From its definition, a formative construct is defined through its measurement items [14] such that changing one of the items would yield a changed construct. Unlike the reflective constructs, the items of a formative measure are supposed to tap into different aspects of the construct in order to "cover" the entire construct. Hence, the measures are not required to and often not intended to covary.

Multi-dimensional constructs are modeled as a composite of its sub-constructs where the construct is defined through its sub-constructs. Each sub-construct may in turn be modeled as either reflective, formative or multidimensional. Thus, measuring a multidimensional construct means to combine the measures of all its sub-constructs, representing a kind of divide-and-conquer strategy to modelling.

4.2 A risk perception model

The model of risk perception we propose is based on the concepts identified in common risk analysis frameworks and previous research on risk perception. The model is depicted in Fig. 4. Below, we describe the different constructs of the model and suggest which type of construct would be appropriate. Determining the correct type of construct depends on the purpose of the model and of course how it is intended to be measured. Thus, it may be perfectly sensible to model the constructs of our model differently, if the purpose was different.

Risk is in current literature and among security professionals typically defined as the combination of likelihood and impact (see Section 3). If we were to model risk as reflective, the corresponding measure would have to be on the form *"How risky is it to ... ?"*. There would be no way to capture the likelihood and impact of

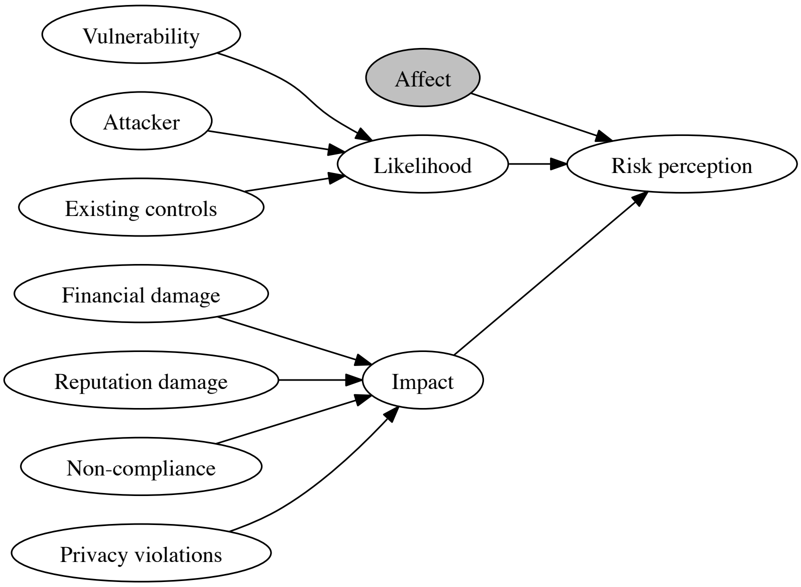

Fig. 4: Concepts of information security risk

a threat. Thus, for our purposes, it is evident that risk should either be formative or multi-dimensional. The difference between these two types are more subtle, since it really depends on whether affect, likelihood and impact are just three measures that jointly form risk perception, or if they are seperate constructs to be measured on their own. As we base ourselves on the concepts of risk analyses, we believe the latter to be the case and hence model risk perception as a multidimensional construct.

The concept of *affect* is commonly viewed in risk perception literature as the *"experienced feeling states associated with positive or negative qualities of stimulus"* [32, p. 4]. Although seldom explicitly labeled as such, it is typically assumed to be reflective. That is, measuring feelings such as fear or worry all tap into the same aspects of a concept (the negative qualities).

Likelihood is similar to risk perception in that there are different concepts that make up the likelihood (Fig. 4). However, a notable difference is that likelihood is not commonly defined as the combination of the vulnerabilities, attackers and existing controls. These three concepts influence the likelihood, although not necessarily simultaneously. I.e., it is perfectly conceivable that there may exist serious vulnerabilities and no motivated or skilled attackers at the same time. Thus, the vulnerabilities, attackers and existing measures are not required to covary and hence a formative or multi-dimensional construct seems appropriate. For multi-dimensional constructs it is assumed that the sub-constructs themselves are distinct [14], so that measurements of each sub-construct do not capture each other. In other words, there should be a clear and definite separation between the sub-constructs. Vulnerabilities and existing security measures do however have commonalities even though the concepts themselves are not identical. E.g., the lack of a security measure may increase the vulnerability. Similarly, vulnerabilities and attacker motivation/skill also share some of the ideas. A vulnerability that is easy to exploit would not require the attacker to be very skillful, and hence the two concepts also tap into one another. Therefore, it appears that modeling likelihood as a formative construct may be the better option, such that vulnerabilities, attackers and existing controls denote different aspects of likelihood, rather than complete constructs of their own.

Impact is perhaps the most difficult concept to model, because it depends to a large extent on the threat in question and the context in which it exists. If we are considering the threat of credit card fraud against individual users, it safe to assume that reputation damage is not relevant. However, if we are considering the same threat from the perspective of a payment company, then the reputation damage may be very relevant. The possible impacts (financial damage, reputation damage, non-compliance and privacy violation) in our model are by no means exhaustive, there could be several other impacts that are important for the context at hand. We have previously shown [22] that users collaborating across company borders are focused on the loss of competitive advantage impact. Thus, the aspects of impact that we list in Fig. 4 are to be treated as a starting point on which context-dependent impact aspects may be added. Since there is no reason to assume that the different possible impacts covary, it does not seem appropriate to model the construct as reflective. Further, it is also noted that financial damage and reputation damage may overlap, in the sense that damage to ones reputation yields reduced sales and thus financial loss. Therefore, we suggest that the impact construct be regarded as a formative construct.

4.3 An instrument for measuring risk perception

The motivation for modelling risk perception is to devise a measurement framework that can more accurately capture the risk perception of regular users. For this, we propose a self-report questionnaire to let users respond to statements regarding the risk of specific ICT threats. Here we present a preliminary sketch of the instrument, currently with excessive redundancy in the questions. Readers should take care not to treat any of these questions as tested and verified.

In Table 2 we have listed some example questionnaire items for measuring two of the sub-constructs of risk perception; likelihood and impact. The statements are supposed responded to by indicating the degree to which respondents agree with the statements (e.g.on a five-point scale from *"strongly agree"* to *strongly disagree*). Since risk perception is modeled as a multi-dimensional construct, there are no measurement items for the risk perception itself. Instead, it is to be computed from its sub-constructs, which in turn are measured through their supporting concepts rather than directly. Hence, we have not included questions

Table 2: Example questionnaire items for the multi-dimensional risk perception construct

Construct	Concept	Statement/Question
Likelihood	Vulnerability	*"Exploiting vulnerability is easy"* *"The vulnerability is well known"*
	Attacker	*"Attackers have the necessary skills to exploit the vulnerability"* *"Attackers have financial interest in exploiting the vulnerability"*
	Existing controls	*"Existing security measures prevent attackers from exploiting the vulnerability"* *"Existing security measures can detect attackers exploiting the vulnerability"*
Impact	Financial damage	*"Attackers exploiting vulnerability would result in financial damage"*
	Reputation damage	*"Attackers exploiting the vulnerability would damage the company's reputation"*
	Privacy violation	*"Attackers exploiting the vulnerability would cause a breach of customer's privacy"*

or statements directly targeting likelihood for instance. The example questionnaire items do not include measures of affect, as there are several tested and validated measurement instruments that can be used (e.g., Crites et al. [5]).

What becomes apparent when creating measurement instruments is that the threat and potential impact must be specified to a certain detail. It is difficult to say anything about attacker motivation, unless you know who the attacker is. Thus, for the risk perception measure to work, there needs to be a serious effort up front to determine the possible attackers, vulnerabilities, threats and the possible resulting impact. However, by expanding and extending this framework of risk perception measures, the effort required for adapting measurement instruments will steadily decline.

5 Discussion

In this section we discuss some of the difficult issues of validity and trust.

5.1 Construct validity

A central aspect to any model and measurement is their validity. Does the model actually represent risk perception? Does the measurement actually measure risk perception? Both the model and the measures are based on extensively used and agreed-upon concepts for conducting risk analysis. Our risk perception model is therefore tightly coupled with the information security communities definition of risk. The central point here is whether the concepts of risk analysis can meaningfully be applied to risk perception. Or to put it in other terms: Do people actually consider attackers' motivation as part of their risk perception? In our experience regular users often refer to possible attacker motivations or skills. Statements like *"who would want my information"* or *"it is very difficult to make use of our source code"* are indeed not uncommon and clearly demonstrate that users consciously consider the motivation and skills of potential attackers.

Another thing to consider is that the systematic approach of risk analysis attempts to identify objective risk, that is free from subjective judgments. That is, risk analysis is supposed to trigger the rational system, not the intuitive system. Whereas our risk perception measure also consider affect or intuition. A central concept in the *risk as feelings* theory (see Section 3) is the mutual relationship between the cognitive and affective response to risk. That is, that the rational system both influence and is influenced by the intuitive system.

Our model and corresponding instrument for measuring risk therefore have a sound basis in theory. It is worth noting that the measurement instrument needs to be tested and properly evaluated before definitive statements can be made regarding the validity of the constructs.

5.2 Content validity

A potential problem with our framework is that it requires identification of the specific threats, vulnerabilities, attackers and potential damages to be assessed. We have already discussed the implications of this in terms of reusing measurement instruments and the effort required to identify and prioritize the concepts. However, a perhaps more severe problem is the potential threat to validity it poses. That is, how do we know that the identified threats, vulnerabilities, attackers and potential damages are appropriate and sufficient? It may be that an important group of attackers are omitted or disregarded from the measurement instrument, which again may give an invalid result. This may happen even if the the statements (or scale items) used have previously been tested and verified. This further strengthens our belief that a risk perception measure should be treated as a starting point and would require great care to address the validity concerns when applied to other contexts..

5.3 Convergent and discriminant validity

Our model, constructs and corresponding measures are supported by existing theory and practice. However, it is common to test a new measure for convergent and discriminant validity. That is, to ensure that our measure of risk correlates with other measures that it theoretically should correlate with, while at the same time be unrelated to other measures that theoretically should be unrelated.

However, there are no well established measures of risk perception other than the pure reflective measure risk commonly used (see related work in Section 2). We have postulated that these measures are not particularly good for ICT risk perception as they are too abstract to meaningful for our purposes. Normally one would have liked our measure to have high convergent validity with these other risk perception measures. However, this may indicate that our measure is equally poor as the existing ones. On the other hand, if our measure and the other measures demonstrate discriminant validity (they are unrelated) that could would indicate that one of the measures are invalid, but not which one.

Another method to indicate such validity would be to measure risk perception in relation to another construct. The protection motivation theory for instance postulates that there is a relation between the perceived risk and the intention to use protective technology. Hence, if our measure fits such a model, it would strengthen the argument that the measure is indeed valid.

5.4 Relation to trust

Risk perception is to some extent related to trustworthiness and trust. There are several trust models that incorporate risk [15], and intuitively trust also imply a certain degree of risk. However, as noted by Mayer, Davis and Schoorman [21], risk is an outcome of trust and therefore "differentiates the outcomes of trust from general risk-taking behaviors because it can occur only in the context of a specific, identifiable relationship with another party" [21]. Since we propose a general purpose adaptable instrument for risk perception measurement, we have omitted trustworthiness as part of our risk perception. However, in specific contexts where there are indeed identifiable relationships between parties, trustworthiness may well be included as a factor that affect risk perception.

6 Conclusion

In this paper we have presented a risk perception model and a preliminary measure of the risk perception of ordinary ICT users. Our approach is based on a combination of *prior research* on general risk perception and *common practices* in the risk analysis field. The risk perception measure focus on measuring aspects on which ordinary users can be expected to have an opinion. The validity of the construct is promising since it is based on solid existing theory and practice. However, great care should be taken to address the threats to content validity for different risks.

In further work we will employ our instrument in a larger study, testing the validity of our risk perception measure in a larger population.

References

1. Bélanger, F., Carter, L.: Trust and risk in e-government adoption. The Journal of Strategic Information Systems 17(2), 165 – 176 (2008)
2. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3), 523–548 (2010)

3. Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R.: Introducing octave allegro: Improving the information security risk assessment process. Technical report CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University (May 2007)
4. Chenoweth, T., Minch, R., Gattiker, T.: Application of protection motivation theory to adoption of protective technologies. In: System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on. pp. 1 –10 (jan 2009)
5. Crites, S.L., Fabrigar, L.R., Petty, R.E.: Measuring the affective and cognitive properties of attitudes: Conceptual and methodological issues. Personality and Social Psychology Bulletin 20(6), 619–634 (1994)
6. Crossler, R.: Protection motivation theory: Understanding determinants to backing up personal data. In: System Sciences (HICSS), 2010 43rd Hawaii International Conference on. pp. 1 –10 (jan 2010)
7. Epstein, S.: Integration of the cognitive and the psychodynamic unconscious. American Psychologist 49(8), 709–724 (Aug 1994)
8. Featherman, M.S., Pavlou, P.A.: Predicting e-services adoption: a perceived risk facets perspective. International Journal of Human-Computer Studies 59(4), 451 – 474 (2003)
9. Finucane, M.L., Alhakami, A., Slovic, P., Johnson, S.M.: The affect heuristic in judgements of risks and benefits. Journal of Behavioral Decision Making 13(1), 1–17 (January 2000)
10. Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B.: How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. Policy Sciences 9, 127–152 (1978), 10.1007/BF00143739
11. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18(2), 106–125 (April 2009)
12. Horst, M., Kuttschreuter, M., Gutteling, J.M.: Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in the netherlands. Computers in Human Behavior 23(4), 1838 – 1852 (2007)
13. ISO/IEC 27005: Information technology — Security techniques — Information security risk management. International Organisation for Standardisation, Geneva, Switzerland (2011)
14. Jarvis, C.B., MacKenzie, S.B., Podsakoff, P.M.: A critical review of construct indicators and measurement model misspecification in marketing and consumer research. Journal of Consumer Research 30(2), 199–218 (September 2003)
15. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision Support Systems 43(2), 618 – 644 (2007)
16. Kahneman, D.: A perspective on judgment and choice: Mapping bounded rationality. American Psychologist 58(9), 697–720 (Sep 2003)
17. Kahneman, D., Frederick, S.: Representativeness revisited: Attribute substitution in intuitive judgment. In: Gilovich, T., Griffin, D., Kahneman, D. (eds.) Heuristics and biases: The psychology of intuitive judgment, pp. 49–81. Cambridge University Press (2002)
18. Kim, D.J., Ferrin, D.L., Rao, H.R.: A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems 44(2), 544 – 564 (2008)
19. Loewenstein, G.F., Weber, E.U., Hsee, C.K., Welch, N.: Risk as feelings. Psychological Bulletin 127(2), 267–286 (2001)

20. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer-Verlag (2011)
21. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. The Academy of Management Review 20(3), pp. 709–734 (1995)
22. Nyre, Å., Jaatun, M.: Usage control in inter-organisational collaborative environments – a case study from an industry perspective. In: Quirchmayr, G., Basl, J., You, I., Xu, L., Weippl, E. (eds.) Multidisciplinary Research and Practice for Information Systems, Lecture Notes in Computer Science, vol. 7465, pp. 317–331. Springer Berlin / Heidelberg (2012)
23. Nyre, Å.A., Jaatun, M.G.: On the adoption of usage control technology in collaborative environments. In: Proceedings of the 12th International Conference on Innovative Internet Community Systems. pp. 142–153. Trondheim, Norway (June 13-15 2012)
24. OWASP: OWASP testing guide v3. Tech. rep., The Open Web Application Security Project (2008), `https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf`
25. Pavlou, P.A.: Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce 7(3), 101–134 (April 2003)
26. Petter, S., Straub, D., Rai, A.: Specifying formative constructs in information systems research. MIS Q. 31(4), 623–656 (December 2007)
27. Rogers, R.W.: A protection motivation theory of fear appeals and attitude. Journal of Psychology 91(1) (1975)
28. Siponen, M., Pahnila, S., Mahmood, A.: Employees' adherence to information security policies: An empirical study. In: New Approaches for Security, Privacy and Trust in Complex Environments, LNCS, vol. 232, pp. 133–144. Springer Boston (2007)
29. Sjöberg, L., Moen, B.E., Rundmo, T.: Explaining risk perception: An evaluation of the psychometric paradigm in risk perception research. Rotunde 84, Norwegian Univeristy of Science and Technology (2004)
30. Slovic, P.: Perception of risk. Science 236(4799), 280–285 (April 1987)
31. Slovic, P., Fischhoff, B., Lichtenstein, S.: Rating the risks. Environment 21(3), 14–20,36–39 (1979)
32. Slovic, P.: The Feeling of Risk - New perspectives on risk perception. Earthscan, London, UK (2010)
33. Slovic, P., Finucane, M.L., Peters, E., MacGregor, D.G.: Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. Risk Analysis 24(2), 311–322 (2004)
34. Slovic, P., Finucane, M.L., Peters, E., MacGregor, D.G.: The affect heuristic. European Journal of Operational Research 177(3), 1333 – 1352 (2007)
35. Slovic, P., Fischhoff, B., Lichtenstein, S.: Why study risk perception? Risk Analysis 2(2), 83–93 (1982)
36. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology (2002)
37. Woon, I., Tan, G., Low, R.: A protection motivation theory approach to home wireless security. In: Proceedings of the Twenty-Sixth International Conference on Information Systems. pp. 367–380 (2005)