Perceptual Influences on Risk Assessments and the Challenges for Information Security and Network Management

William Knowles, Daniel Prince and David Hutchison
Lancaster University, Lancaster, UK
{w.knowles, d.prince, d.hutchison}@lancaster.ac.uk

***Abstract*—The responsibility for information security, or more accurately, information assurance, permeates throughout all facets of modern organisations, and consequently encompasses a variety of stakeholders (i.e., lay people), each with their own perceptions as to the value, and risks to this information. Although a wide range of disciplines have provided important contributions to our understanding of the way that people perceive risk, this paper will predominantly focus on psychological explanations, in order to examine the disparity between lay and expert perceptions of risk, and what impact this has upon an information security risk assessment in terms of both data collection, and the recommendation of countermeasures.**

I. Introduction

Does risk exist independently and can it be given an objective measure, or can a subject's perception of risk (even if it is considered a misconception by risk experts) be a reality? Despite the assumptions of a quantifiable, objective measure of risk that is made in risk assessments, the literature of the social sciences has largely abandoned this notion. The argument is now that although there can be seen to be objective facts (e.g., the number of USB sticks lost in a year), the notion of risk is a human construct that coincides with its perception, and that it therefore contains a high degree of subjectivity [1].

The origins of structured risk assessment can be traced back to the Asipu, a group of quasi-risk consultants that lived in the Tigris-Euphrates valley of Ancient Babylonia around 3200BC. For the Asipu, there was no subjectivity, but only authoritative and incontrovertible readings of the signs of the Gods [2]. Modern risk assessments are laboured with the challenge of operating with non-celestial and more practical methodologies, while fitting into the broader framework of risk management. Although risk management is an ongoing process, risk assessment forms a snapshot of assessed risk for a specific time period and parametrises the entire risk management process. This relationship is illustrated in Figure 1.

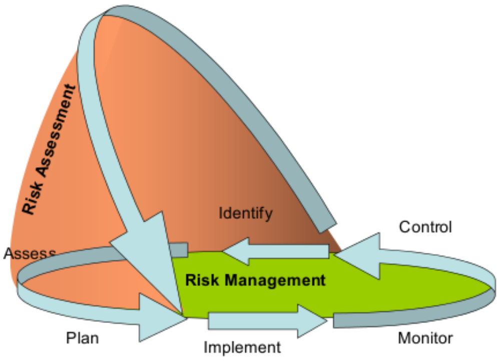

Fig. 1. The Risk Management-Assessment Relationship [3]

Although there are a number of methods and tools for approaching risk assessments, from those for public bodies (e.g., CRAMM) to de facto standards (e.g., OCTAVE) they can all be considered variations of a consolidated number of steps: (i) asset identification and valuation against the confidentiality, integrity, and availability (CIA) triad, (ii) vulnerability assessment, (iii) threat assessment, (iv) risk evaluation, and (v) the recommendation of countermeasures. As highlighted by Jones and Ashenden [4], however, the recommendation of countermeasures does not signal the end of the risk assessment process. Risk assessment should be iterative, and accompanied by project plans to aid in the implementation of countermeasures, and the monitoring of their effectiveness. All aspects of this risk assessment process are pervaded by subjectivity, due to judgements (both lay and expert) at all of its stages, from the definition of scope, to the psychological and knowledge profiles of subjects determining which vulnerabilities are known versus those that are unknown [5], to the estimation of a particular exposure, and so on [6].

The extent to which this subjectivity pervades risk assessment makes a step-by-step discussion of its impact far beyond the limitations of this paper. The remainder of this paper will, however, address the factors that can affect the data collection process (predominantly in threat assessments), and what this means for the recommendation of countermeasures.

II. Risk Perception and the Risk Assessment Process

The subjective judgement of a risk and its severity is called risk perception. It is now a well established argument within the risk perception literature, that risk experts and lay people differ systematically in their perceptions over what constitutes a risk, and to their level of exposure [7]. The perceptions of risk experts have been shown to follow a stricter rationality than those of lay people, and that these perceptions correlate highly with the breadth of statistical measures used in formal

ISBN: 978-1-902560-26-7 © 2012 PGNet

risk assessments [8]. Conversely, the perceptions of lay people are considered more irrational [9], and are heavily influenced by individual traits and sociocultural factors (e.g., education and political orientation), with "peer opinion, hearsay, and media coverage a substitute for insufficient personal experience or knowledge"[10].

It should be noted that the rationality of risk experts is only strict, and not perfect. The perceptions of risk experts have been shown to differ within specialisms, as with the differences in standards of acceptable evidence [11], and also between specialisms, as risk experts make judgements about risks outside of their field of expertise with no better accuracy than lay people [12]. However, their judgements remain significantly more accurate than lay people. Despite this, any discussion of risk perception within the risk assessment process must be aware of this factor, in a large part due to the number of informal judgements that risk experts must make.

The aforementioned permeation of subjectivity throughout the risk assessment process is accompanied by this disparity between expert and lay risk perceptions, and it is from this disparity that the perceptual factors create situations for inaccurate judgements to be made. These factors serve to amplify or attenuate risk perception, but the way in which the risk-benefit trade-off is gauged is through the employment of cognitive heuristics, or when incorrect judgements are made, cognitive biases. Cognitive heuristics represent simplistic interpretations of risk judgements. People utilise cognitive heuristics when quantifying probabilities and consequences, because their cognitions rarely function in a comparable manner to the statistical methods of risk assessments [13]. The literature of psychology contains a multitude of theorised heuristics and biases, which could potentially play a role in any judgements made during data collection in risk assessments, however, there are four of particular significance:

First, and what is widely considered the most important, is the availability heuristic. This heuristic utilises the ease with which an event comes to mind, on the premise that the easier it does, the more likely it has unfolded in such a way in the past, and the more likely it will continue to do so in the future. An availability bias leads to the overestimation of recently manifested risks in a lay person's mind and also of those memorable (and often extremely rare or traumatic) risks [10]. A conspicuous example of the application of the availability heuristic is with the mass media. Frequent exposure to negative topics begets high levels of perceived risk [14], and it is often associated with why lay people have false perceptions about the absolute frequencies of risks.

Festinger's [15] cognitive dissonance theory is a related strand of research to the the availability heuristic (research has of yet, failed to disentangle the roles of cognitive availability and dissonance). Cognitive dissonance theory suggests that people seek consistency in their cognitions, and that any inconsistencies (i.e., dissonances) between beliefs or behaviours are solved by changing one or the other, and that this is usually the beliefs to accommodate the behaviour. For example, lay people (e.g., managers) underestimating the dangers of breaching data classification policies (e.g., in order to reduce their workload) because it reduces the state of dissonance caused by employing dangerous working habits.

Second, the representative heuristic, which involves estimating the likelihood of a novel event occurring, by situating the perception of its risk within personal categories of experience and knowledge about safe events. However, the problem for data collection during risk assessments is that this estimation is done without "taking account of other normatively important principles such as its a priori likelihood of occurring (i.e., the base rate)" [13], leading to the possibility of erroneous risk assessments if it becomes a representative bias.

Third, the anchoring heuristic, which involves a person focusing (i.e., anchoring) too heavily on a particular piece of information or value, which can then affect subsequent estimates made during risk assessments. For example, indicating to a person that *n* per cent of fire extinguishers in a building are foam-based, and then asking them how many people they see shoulder surfing through doors to restricted areas in a typical day. This person will usually reply with an irrelevant *n* per cent value [16]. Furthermore, it need not be the risk expert that indicates the initial value, as the anchoring heuristic would also apply to answers to previous questions (i.e., from the lay person).

Fourth, and most recently developed as a result of the work on the psychometric paradigm is the affect heuristic, where perceived risk is based on the way a given situation makes a person feel. Reflexive emotional affects (i.e., for both perceived benefits and risks) towards external stimuli (e.g., threats to information security) that often preclude thought have been shown to be inversely correlated in a subject's mind. For example, higher perceived risk is associated with lower perceived benefits [6]. Furthermore, negative stigma (possibly subconsciously) can become attached to certain events, exacerbating the complexities of attempts to achieve objective data collection in risk assessments [17].

When analysing data relating to lay perceptions and judgements, risk experts must also consider what makes a risk acceptable (if this is even possible). Discussion over what constitutes an acceptable risk has its origins with Starr's [18] revealed preference concept, which was proposed after developing a framework for weighing technological risks against their benefits. Starr argued that society had through a process of trial and error, reached an "essentially optimum" equilibrium between risk and benefit, and that societal risk acceptability of new risks could be inferred through study of historical data on accepted risks. Starr argued that risk acceptability was roughly proportional to the third power of its benefits, and highlighted the role played by voluntariness, arguing that lay people would willingly accept risks from voluntary activities containing threats up to 1000 times as great than for involuntary threats (even if the activities provided the same level of benefits). Slovic [19] highlights how "concerns about the validity of many of the assumptions inherent in the revealed preferences approach stimulated" the expressed preferences approach, which laid the foundations of the psychometric paradigm. The expressed preference approach utilises psychometric scaling and analysis across a multitude of dimensions (initially it was 9, but then later expanded to 18) on the premise that "direct questioning of [lay] people regarding their attitudes towards risks and benefits associated with various activities... captures values that reflect present attitudes rather than past preferences" [20]. The expressed preference approach demonstrates that "people focus on the qualitative aspects of risk situations not modelled in formal assessments, and this can lead to important and predictable differences between their evaluations and those derived from formal assessments" [13]. However, these aspects of perception remain quantifiable and predictable [19], and can be mapped over two factors that account for between 70 and 90 percent of the variance between lay and expert risk perceptions [21]:

First, is the dread factor, which is associated with risk aspects surrounding the degree of aroused feelings of dread, risk uncontrollability, irreversibility, threat to future generations, and potential to be globally catastrophic [22]. Camp [16] argues that the lack of dread is one of the reasons that information security is often systematically underrated (i.e., because information loss is not considered frightening). Furthermore, it provides some explanation of why internal information security threat-agents (e.g., malicious insiders) are considered less serious and paid less attention than external information security threat-agents [23]. For example, in most cases, network security is less understood than physical security, and is therefore perceived to be a greater threat (e.g., from the unknown and unobservable outsider), despite most threats originating internally where people have significant physical exposure to information.

Second, is the unknown factor, which is associated with risk aspects surrounding its observability, unfamiliarity (i.e., both to lay people and scientists), novelty, and the extent of delayed affects [22]. Regardless of the scientific metrics produced by formal risk assessment, people judge threats that they perceive to be high on these aspects to also be high in risk. The influence of the unknown factor aids in explaining why people willingly expose themselves to certain high-risk threats (as determined by risk assessments), while being averse to those that could be deemed to be low-risk [13].

In the pioneering work on the psychometric paradigm, the factor representing the number of people exposed to a threat was also seen to play a large role in the variance of lay and expert risk perceptions (Slovic, 1987). Furthermore, in more recent research a fourth factor has been highlighted, which concerns notions of morality and tampering with nature [14]. This is exemplified over temperamental lay concerns surrounding specific types of information that must be secured (e.g., children's medical records), which may given resources at the expense of more serious risks.

One pitfall of this research into the cognitive factors of risk perception is that it largely ignores motivation in the choice of acceptable behaviours. This is demonstrated in how lay people, despite often having adequate knowledge of relative risk, change their perceptions of personal risk as they apply this knowledge to their own behaviour [7]. This perception-personal behaviour nexus has led to research focusing on the role of comparative risk, which is concerned with lay tendencies to proclaim below average exposures to risk than their comparative peers (e.g., see [24]). Rothman et al [25] suggests that this is a result of a social comparison process, where people overestimate peer risk, rather than underestimate personal risk, in part due to an optimism bias. For risk assessments, this variable could possibly be extrapolated to the project grouping and functional departmental levels as each considers its risk exposure to be lower than their comparative peer groupings.

Issues surrounding the subjectivity in risk assessments are further exacerbated when their scope is expanded beyond an organisation's functional divisions, and perceptual differences are considered between an organisation's strategic business units (SBUs), and in both their upstream and downstream supply chains. For example, because risk perception has been shown to differ between groups (e.g., different cultures) [26]. Each SBU or organisation within a supply chain will be uniquely marked by its own organisational culture and behavioural norms, which influence their respective employees' perceptions of what constitutes a risk. It should be noted that this could also apply to cultural differences between lay people within the same groups (e.g., functional divisions or project teams). However, group division by culture (conventional or organisational, or both) especially between geographically distant regions exacerbates and reinforces other variables that could affect the risk assessment process. For example, research by Hsee and Weber [26] argues that a culture's position on the individualism-collectivism continuum (i.e., which do they intrinsically promote) will affect the degree of riskiness that members perceive about objects or events as "collectivism cushions in-group members against the consequences of negative outcomes".

Psychological, social, cultural, and a multitude of other factors have all been shown to play some role in risk perception, however, it is only in recent years that an integrative theoretical model has been proposed. This model has come to be known as the social amplification of risk framework (SARF) [27]. The SARF proposes that initial events (e.g., an organisation punished from breaching Data Protection laws) are neglected until communicated. The communication process occurs as information is passed through various social agents (e.g., the media) at multiple levels who amplify it (e.g., through it being perceived as having high levels of dread), or attenuate it (e.g., through having trust in the communicator) [13]. The secondary, tertiary, and so on effects of this communication process can have a wide variety of direct consequences (e.g., in terms of legislation) and indirect consequences (e.g., on wider risk perception). Most significantly, the SARF highlights that risk perception is a result of the processes of acquisition and interpretations of communicated risk [27]. However, as highlighted by Kasperson and Kasperson [28], risk assessments are judged by their accuracy, but lay people evaluate risk communications in terms of their adaptivity to their existing perceptions. This can mean, for example, that during threat assessments, threat-agents can be amplified to such an extent that it distorts the true threat that they present.

Contextual factors, therefore, also have implications in any attempt to achieve the most objective data as possible during data collection. For example, when conducting both qualitative and quantitative assessments, the way that the questions are framed will play a significant role in sculpting an individual's risk perception construct. Levin et al [29] proposed a typology of framing effects, which could all be considered to lead to bias in risk perceptions: risky choice framing, goal framing, and attribute framing. Each of these framing effects has different effects (e.g., positive risky choice framing generating a bias towards risk-averse behaviour), however, they all demonstrate that the way information is framed (including questions) can lead to perception reversals.

This paper has so far focused on the inherent complexities that risk perception places upon varying stages of risk assessments that involve data collection and analysis. However, risk perception must also be considered in the choice of the recommended countermeasures, and the manner to communicate the findings and recommendations in a way that is most likely to achieve a successful implementation.

Although the term lay person carries derogatory connotations of lower-rung organisational hoi polloi, the impact of risk perception on the risk assessment process includes those in managerial positions (including those at board level). This is particularly significant considering that managers will be extensively involved in any risk assessment process (e.g., for detailing organisational process, and having an even more prominent role in risk assessments with limited funding). Lay people (at board-level) also, therefore, with their irrational risk perceptions will ultimately be responsible for the choice of countermeasures. If the findings and recommendations are not communicated effectively, it can lead to support for ineffective risk control measures [30]. This is a challenging position for risk experts as lay people have been shown to often misinterpret information in both quantitative assessments and qualitative assessments, and are largely unresponsive to technocratic risk communication (i.e., through statistics and probabilities) in general [23]. For example, Berry et al [31] demonstrated that risk experts interpret a label of "very rare" as 0.1 percent, while conversely, lay people interpreted this as 4 percent. As lay people ultimately choose countermeasures, this can lead to support for risk controls that support their own erroneous risk perceptions, opinions, or business goals, or support risk controls that play to the wider public's perception of risk (e.g., to improve business). For example, there is an abundance of literature on the over-optimism of managers [32], and research suggests that managers have difficulty processing ambiguous and low probability risks. Hodgkinson and Starbuck [13], for example, from an analysis of confidential statistics on information security, argue that management frequently overcommit resources to high probability (and visibility) threats (e.g., hackers), and under-commit to those of low probability (e.g., information systems with low tolerance during periods of peak demands), despite holding formal statistics on the cause of the threat to losing information availability.

One consideration of an effective countermeasure is cost, and the cost-benefit analysis for each countermeasure must include the operational cost of a successful implementation at all organisational levels. This requires a greater understanding of not only what lay perceptions of possible controls are, but why these perceptions are why they are, and the behaviour they produce, in order to leverage these differences into an integrative countermeasure and communication plan [26]. One such approach is to involve a wide selection of stakeholders in risk assessments through a multitude of participatory techniques (e.g., focus groups, consensus workshop) [13], and then to examine the differences in perceptual languages of lay people and risk experts through the use of mental models. A critical discussion of this process, however, is beyond the scope of this paper.

III. Conclusion

The gap between lay and expert perceptions of risk permeates throughout each stage of the risk assessment process, and the complexity and number of associated perceptual vectors presents a serious challenge not only for defining current risk levels, but in the definition of feasible countermeasures. Although the literature on risk perception is well established, research is only beginning to seriously consider the overbearing issues surrounding information security, and there remains little upon its assessment within more holistic contexts (and primarily only with supply chains, e.g., [33] and [34]). The promotion of collaboration and sharing that pervades throughout the information economy constitutes one of the most pressing issues for risk management. Not only are new models and processes having to be developed for information security risk assessments, but they must address the necessities for adopting a wider scope as information becomes increasingly exposed in ubiquitous environments.

IV. Future Work

In order to address the novel security requirements demanded by industrial control systems (ICSs), there has been a rising number of standards, regulations, and guidelines (forthwith referred to as just standards) that have been proposed by various national, international and multilateral initiatives (e.g., ISA-99, NIST SP 800-82, and the CPNI Good Practice Guide). However, despite the unique body of requirements presented by ICSs, the standards used in traditional IT systems continue to utilised extensively in their security management (e.g., the ISO 27000 series). In the protection of any computer system, the development and utilisation of comprehensive metrics is essential to the provision of actuarial quality data. Although there has been progression in the standards for ICSs, the definition of metrics that are to be used to uphold them has not kept pace. As a consequence, metrics defined for traditional IT systems are still used extensively, despite not being directly transferable, due to their original definitions having different goals in mind (e.g., for the CIA triad, when for ICSs it is AIC). One avenue of future work will be to look into the definition of ICS-specific security metrics, and the development of a framework for their collection, conditioning (e.g., through normalisation, categorisation, and prioritisation) and computation, in order to provide some means of performing comparative analyses of the security offered by different ICSs. The outputs of this framework will potentially be utilised by multiple stakeholders for a multitude of purposes, and therefore the requirement for understanding the role played by subjective risk perceptions is implicitly essential to its development.

References

[1] P. Slovic, "Perception of risk posed by extreme events." *Risk Management strategies in an Uncertain World*, Apr. 2002.

[2] V. T. Covello and J. Mumpower, "Risk analysis and risk management: An historical perspective," *Risk Analysis*, vol. 5, no. 2, pp. 103–120, Jun. 1985. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1985.tb00159.x/abstract

[3] "Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools," European Network and Information Security Agency (ENISA), Survey of existing Risk Management and Risk Assessment Methods., Jun. 2006.

[4] A. Jones and D. Ashenden, *Risk management for computer security: Protecting your network and information assets*. Butterworth-Heinemann, Mar. 2005.

[5] E. Anderson, J. Choobineh, and M. R. Grimaila, "An enterprise level security requirements specification model," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. HICSS '05*. IEEE, Jan. 2005, pp. 186c– 186c.

[6] P. Slovic, "Trust, emotion, sex, politics, and science: Surveying the Risk-Assessment battlefield," *Risk Analysis*, vol. 19, no. 4, pp. 689–701, 1999.

[7] J. Pligt, "Cognition, and affect in risk perception and risky decision-making," in *Psychology at the turn of the millennium, social, developmental, and clinical perspectives*, C. V. Hofsten and L. Bckman, Eds. Psychology Press, 2002, pp. 247–270.

[8] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Rating the risks," *Environment: Science and Policy for Sustainable Development*, vol. 21, no. 3, pp. 14–39, 1979.

[9] A. Plough and S. Krimsky, "The emergence of risk communication studies: Social and political context," *Science, Technology, & Human Values*, vol. 12, no. 3/4, pp. pp. 4–10, 1987. [Online]. Available: http://www.jstor.org/stable/689375

[10] J. J. L. M. Bierens and M. t. R. v. Drenkelingen, *Handbook on drowning: prevention, rescue treatment*. Birkhuser, Nov. 2005.

[11] K. Schaffner, "Causing harm: Epidemiological and physiological concepts of causation," in *Acceptable Evidence: Science and Values in Risk Management*, D. Mayor, Ed. Oxford University Press, USA, 1994, pp. 204–217.

[12] R. P. Barke and H. C. JenkinsSmith, "Politics and scientific expertise: Scientists, risk perception, and nuclear waste policy," *Risk Analysis*, vol. 13, no. 4, pp. 425–439, Aug. 1993. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1993.tb00743.x/abstract

[13] G. P. Hodgkinson and W. H. Starbuck, *The Oxford handbook of organizational decision making*. Oxford Handbooks Online, May 2008.

[14] L. Sjberg, "Factors in risk perception," *Risk Analysis*, vol. 20, no. 1, pp. 1–12, Feb. 2000. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.00001/abstract

[15] L. Festinger, *A Theory Of Cognitive Dissonance*. Stanford University Press, Jun. 1957.

[16] L. J. Camp, "Mental models of privacy and security," *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, 2009.

[17] J. Flynn, P. Slovic, and H. Kunreuther, *Risk, media, and stigma: understanding public challenges to modern science and technology*. Earthscan, 2001.

[18] C. Starr, "Social benefit versus technological risk." *Science*, vol. 165, pp. 1232–1238, 1969.

[19] P. Slovic, "Perception of risk," *Science*, vol. 236, no. 4799, pp. 280–285, Apr. 1987. [Online]. Available: http://www.sciencemag.org/content/236/4799/280

[20] I. J. Gabriel and E. Nyshadham, "A cognitive map of people's online risk perceptions and attitudes: An empirical study," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, Jan. 2008, pp. 274–274.

[21] Y. Murakami, *Toward a peaceable future: redefining peace, security, and kyosei from a multidisciplinary perspective*. Thomas S. Foley Institute for Public Policy and Public Service, 2005.

[22] A. Columbus and F. Columbus, *Advances in psychology research, Volume 36*. Nova Publishers, 2005.

[23] G. Stewart, "A safety approach to information security communications," *Information Security Technical Report*, vol. 14, no. 4, pp. 197–201, Nov. 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S136341271000004X

[24] F. W. van der Velde, J. van der Pligt, and C. Hooykaas, "Perceiving AIDS-related risk: Accuracy as a function of differences in actual risk." *Health Psychology*, vol. 13, no. 1, pp. 25–33, 1994. [Online]. Available: http://psycnet.apa.org/?fa=main.doiLandingdoi=10.1037/0278-6133.13.1.25

[25] A. J. Rothman, W. M. Klein, and N. D. Weinstein, "Absolute and relative biases in estimations of personal risk1," *Journal of Applied Social Psychology*, vol. 26, no. 14, pp. 1213–1236, Jul. 1996. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.1996.tb01778.x/abstract

[26] E. U. Weber and C. Hsee, "Cross-Cultural differences in risk perception, but Cross-Cultural similarities in attitudes towards perceived risk," *Management Science*, vol. 44, no. 9, pp. 1205–1217, 1998, ArticleType: research-article / Full publication date: Sep., 1998 / Copyright 1998 INFORMS.

[27] N. F. Pidgeon and R. E. Kasperson, *The Social Amplification of Risk*. Cambridge University Press, Jul. 2003.

[28] J. X. Kasperson and R. E. Kasperson, *The Social Contours of Risk: Publics, risk communication and the social amplification of risk*. Earthscan, May 2005.

[29] I. P. Levin, S. L. Schneider, and G. J. Gaeth, "All frames are not created equal: A typology and critical analysis of framing effects," *Organizational Behavior and Human Decision Processes*, vol. 76, no. 2, pp. 149–188, Nov. 1998. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0749597898928047

[30] A. Bostrom, "Risk perceptions: Experts vs. lay people," *Duke Environmental Law & Policy Forum*, vol. 8, p. 101, 1997. [Online]. Available: http://www.law.duke.edu/shell/cite.pl?8+Duke+Envtl.+L.++Pol+pdf

[31] D. Berry, *Risk, Communication and Health Psychology*. Open University Press, 2004.

[32] D. Lovallo and D. Kahneman, "Delusions of success. how optimism undermines executives' decisions." *Harvard business review*, vol. 81, no. 7, pp. 56–63, Jul. 2003.

[33] G. A. Zsidisin, *Supply chain risk: a handbook of assessment, management, and performance*. Springer, 2008.

[34] S. Barth, *Managerial Perception and Assessment of Catastrophic Supply Chain Risks: An Empirical Study*. GRIN Verlag, 2011.