DOI
https://doi.org/10.18690/um.fov.4.2026.10

ISBN
978-961-299-152-4

Fifty Shades of Orange: Construal Levels, Cognitive Biases, and The Amber Dilemma in Cybersecurity Risk Communication

Gulet Barre,[1] Dinh Khoi Nguyen,[2] Tim Huygh,[1] Arno Nuijten[1, 3, 4]

[1] Open University of the Netherlands, Faculty of Science, Limburg, the Netherlands
gulet.barre@ou.nl, tim.huygh@ou.nl, arno.nuijten@ou.nl
[2] University of Jyväskylä, Faculty of Information Technology, Jyväskylä, Finland
khoi.d.nguyen@jyu.fi
[3] Erasmus University Rotterdam, Erasmus School of Accounting and Assurance, Rotterdam, the Netherlands
arno.nuijten@ou.nl
[4] University of Pretoria, Faculty of Economic and Management Sciences, Department of Auditing, Pretoria, South Africa
arno.nuijten@ou.nl

Board-level decisions on cybersecurity risks are strongly shaped by how information is communicated. Traffic light reporting offers simplicity, but especially the amber light leads to inconsistent interpretations. This paper applies Construal Level Theory (CLT) to explore how psychological distance structures risk responses. Based on interviews with 11 CISOs, we focus on four exemplary biases arising from psychological distance in board-level risk perception. Our results indicate that these biases are not random flaws in judgement but patterned outcomes of directors' and executives' construal levels, influencing whether risks are seen in abstract or concrete terms. Our contribution lies in applying CLT to cybersecurity governance, demonstrating how psychological distance shapes board-level biases, and highlighting how CISOs can manage psychological distance through framing and narrative to support more balanced decision-making. Future work will conduct additional CISO interviews and design an experiment to test how psychological distance shapes board responses to amber risk signals.

Keywords:
cybersecurity communication, cognitive biases, psychological distance, construal level theory, cybersecurity governance, risk reporting

University of Maribor Press

1 Introduction

In the domain of cybersecurity governance, decision-making at the board level often depends on how risks are framed, communicated, and interpreted (Noh et al., 2025; Turel & Bart, 2014). More broadly, recent research highlights that organisational cybersecurity increasingly depends on behavioural and human-centred factors beyond purely technical controls (Barre, 2025). A widely used method for simplifying complex information, such as information about cybersecurity in an organization, is traffic light reporting, in which risks are color-coded as red (indicating high-risk domains), green (indicating low to no-risk domains), or amber (indicating domains whose risk levels are neither high nor low). While red and green are relatively clear, the amber light is more ambiguous, as it indicates that a risk is neither clearly urgent nor fully absent. This ambiguity creates a recurring interpretive tension in board-level decision-making. Construal Level Theory (CLT), developed by Trope and Liberman (2002, 2010), explains how people mentally interpret events at different levels of abstraction depending on psychological distance, that is, how far an event is perceived in time (temporal distance), space (physical distance), likelihood (hypothetical distance), or social connection (social distance). Events perceived as distant are processed more abstractly focusing on why they matter in terms of desirability, whereas events perceived as close are processed more concretely, focusing on how they can be implemented in terms of feasibility. These differences in construal affect not only how risks are understood but also lead to predictable distortions in judgement, known as cognitive biases (Kahneman, 2011).

In the context of cybersecurity governance, these dynamics are particularly important because board members operate at a greater psychological distance from technical operations than CISOs. Boards do not see incident logs, hear the SOC alerts, or manage the patch cycles. Instead, they rely on summaries, dashboards, and interpretations of security operations provided by CISOs. Further, prior research on information security investment demonstrates that board decision-making processes are heavily biased by psychological factors (Dor & Elovici, 2016). However, previous research has paid little attention to how systematic differences in risk interpretation occur, or how they lead to bias in board decision-making.

Our study focuses on four exemplary biases observed in interviews with CISOs, conducted to shed light on the communication of cyber risk to the executive level: optimism bias, pessimism bias, ambiguity bias, and confirmation bias. Each of these can be linked to variations in psychological distance. By applying CLT as a lens, we argue that these biases are not random flaws, but structured patterns shaped by the mental distance between the board and the reality of cyber threats.

This paper contributes to the literature on board-level cybersecurity decision-making by leveraging CLT as a theoretical lens for understanding cognitive biases in cybersecurity governance. Our first contribution is theoretical: we extend the application of CLT into the cybersecurity domain and show that psychological distance systematically structures biases in board decision-making. Second, our empirical contribution lies in analyzing interviews with 11 CISOs, which provide insights into how boards perceive and respond to cyber risks from the perspective of CISOs.

The central research question guiding this study is therefore: How do psychological distance and construal levels contribute to the presence of cognitive biases in board-level cybersecurity risk decisions? By answering this question, we contribute to both theory and practice, expanding CLT into a new organizational domain and offering practical insights for how CISOs can better tailor their communication to reduce bias and improve decision-making at the highest level.

2 Theoretical Background

Construal level refers to the degree of abstraction in how people mentally represent objects, events, or actions. Based on categorization theory (Rosch, 1975) and concept formation (Medin & Smith, 1984), high-level construals are abstract, decontextualized, and focused on goals or meaning, whereas low-level construals are concrete, detailed, and context specific. This distinction helps explain how individuals interpret and act on information differently depending on psychological distance, organizational role, and goals.

In the context of cybersecurity governance, these theoretical insights clarify why board members may perceive, communicate, and respond to cyber risks differently from other stakeholders. People employ higher levels of construal when dealing with

psychologically distant targets (Trope & Liberman, 2010). Psychological distance is a subjective construct, typically defined along four dimensions: temporal, spatial, social and hypothetical. Temporal distance refers to how far in time an event feels, with distant events perceived as less urgent and more abstract. Spatial distance is about how physically far a threat or event feels, making distant events seem less relevant. Social distance refers to emotional or hierarchical separation, with greater distance reducing a sense of personal responsibility. Hypothetical distance relates to how real or likely a situation feels, where uncertain scenarios are often underestimated or ignored (Wakslak et al. 2006).

Besides psychological distance, earlier CLT research has identified several other elements that characterize the effects of high- and low-level construal: desirability & feasibility, hypotheticality, category & exemplar, and pros & cons. These elements are widely recognized as fundamental components of CLT (Trope & Liberman, 2010).

People incorporate both desirability and feasibility considerations when evaluating future actions. According to CLT, actions may be construed in high-level terms, which link them to overarching purposes, or in low-level terms, which connect them to the concrete means of implementation. At higher level of construal, desirability tends to dominate, whereas at lower levels of construal, feasibility becomes more salient. Another dimension is hypotheticality, which concerns the perceived likelihood of future events (Armor and Sackett 2006). CLT suggests that improbable events are construed in abstract, high-level terms, while probable events are construed in concrete, low-level terms. In other words, construal levels become more concrete as the probability of a future event increases. Additionally, category & example addresses the way people mentally represent objects, actions, or events. Under abstract, high-level construal, individuals group these into broader categories, attending to commonalities across instances. Under concrete, low-level construal, they rely on narrower, more specific exemplars that emphasize uniqueness (Liberman et al. 2002). Finally, pros & cons refer to the evaluation of future action based on arguments for or against taking them. At higher levels of construal, positive arguments (pros) tend to become more salient, while at lower levels of construal, negative arguments (cons) are more prominent (Eyal et al. 2004).

Building on the literature on CLT and decision biases in cybersecurity governance, we propose a conceptual model in Figure 1 that links psychological distance to board-level decision-making in the context of cybersecurity governance. The model illustrates that psychological distance shapes the emergence of security-related biases, which subsequently influences how boards evaluate and decide on cybersecurity issues. Therefore, CLT provides a suitable lens to understand how psychological distance contributes to biased risk perception and decision-making at the board level.

Figure 1: Conceptual model

3 Methodology

In an earlier published paper, we conducted a literature review of biases relevant to cybersecurity decision-making (Barre et al., 2025). The literature review resulted in a longlist of decision-making biases relevant to cybersecurity governance. Subsequently, the perceived prevalence of these biases in practice was determined based on interviews with CISOs. Optimism bias was acknowledged by 8 of the 11 CISOs, pessimism bias by 7, ambiguity bias by 10, and confirmation bias by 7. We focus on these four most frequently mentioned biases, while acknowledging that other additional, less prominent biases were also identified during the interviews.

Prior to the main data collection, we conducted a pilot interview with a CISO. The purpose of this pilot was to test the clarity and structure of the interview questions, to assess whether the questions could be addressed within the planned time and to ensure that the terminology was well understood by participants. The pilot interview was not included in the final analysis but served to refine the interview protocol and strengthen the validity of the following interviews.

We conducted 11 semi-structured interviews with CISOs from across Europe. The interview protocol was developed based on existing literature on decision-making biases. Each bias was described in a neutral and non-leading way to avoid influencing responses. We applied the principle of data saturation to determine our stopping point (Guest et al., 2020). Each interview was analyzed for presence of new biases or new associations between biases and one or more CLT dimensions. Data saturation was achieved when the 10th and 11th interviews showed no new categories or linkages, thereby meeting the predefined stop-criterion. Interviews were conducted online and lasted approximately 45 minutes on average.

The interviews offered a balanced perspective from both local and international contexts. 7 CISOs from the Netherlands, 3 CISOs from Belgium and 1 CISO from the United Kingdom. All participants had senior cybersecurity roles in their organizations and had direct involvement in strategic decisions and communications with boards. The majority (10 out of 11) worked in large organizations (250+ employees), while 1 CISO represented a small enterprise with fewer than 50 employees. Professional experience also varied, ensuring perspectives from both seasoned and relatively new CISOs. 3 CISOs have 1-3 years of experience, 2 CISOs have 4-6 years of experience and 6 CISOs have 7+ years of experience. The gender distribution among participants included 3 females and 8 males. The interview protocol covered different components: participants' professional background and experience, their typical ways of reporting cybersecurity risks and communicating with executives, perceived obstacles and complexities in cyber risk communication and examples of how decision biases may manifest in practice. This structure enabled us to link the interview findings to dimensions of CLT.

4 Empirical Illustration of Biases Through the Lens of CLT

In Table 1 below, the rows represent the biases and reporting behavior that CISOs were asked to reflect upon (e.g., optimism bias, pessimism bias, ambiguity bias, confirmation bias and generic amber reporting). The columns represent the different dimensions of psychological distance. If a cell includes a reference such as "CISO#7", this indicates that this particular CISO provides an anecdote that reflects both the bias/reporting theme of that row and the dimension of psychological distance in that column. The table demonstrates that 9 out of 11 CISO provided

anecdotes that contained at least one form of psychological distance when discussing biases and reporting in practice.

Table 2: Mapping psychological distance across biases and reporting behaviours identified by CISOs

Bias	Spatial	Social	Hypothetic	Temporal
Optimism bias		CISO#11	CISO#6	CISO#1
Pessimism bias		CISOs#3; #10	CISOs#5; #10	CISOs#3; #5
Ambiguity bias			CISOs#6; #9	CISO#7
Confirmation bias		CISOs#7; #8	CISOs#7; #8; #9	
Generic (amber) reporting	CISOs#6; #9	CISO#10	CISOs#8; #11	CISOs#6; #7

4.1 Optimism bias

Optimism bias is defined as the tendency to underestimate the likelihood of unfavorable outcomes (Legoux et al., 2014). CISO#1 shared, "They (Board members) ask: 'Why prepare for what hasn't happened yet?'" This illustrates temporal distance. Because board members conceive higher temporal distance, their attention shifts towards broad strategic benefits rather than assessing whether a threat is realistic or urgent. As a result, security investments are forced to compete with other strategic initiatives that appear more immediate and their benefits are perceived more certain than those of abstract cybersecurity threats. Yet, in terms of resilience, trust, and sustained value creation, security investment can be recognized as strategic assets that strengthen organizational competitiveness rather than as purely defensive costs (Kwon & Johnson, 2014).

Similarly, CISO#6 stated, "Because we (the company) passed the audit, they (board members) said: 'I guess we're solid', pointing to hypothetical distance. Passing the audit made the board feel safe, as the risk had already been dealt with. That success made the board perceive the problem as less likely to recur and alleviate the board's uncertainty. While they might not intentionally ignore the risk, the sense of distance made them feel more secure than they probably should have.

In another example, CISO#11 reported: "They (board members) believe our external provider handles everything, so they don't worry much." By shifting responsibility to an external party, the threat appears less personally relevant to the board. Social distance rooted in CLT helps explain how people focus less on whether the threat is still relevant to them.

Taken together, optimism bias increases with greater psychological distance. Temporal distance, when risks are perceived as lying further in the future, and hypothetical distance, when risks are perceived as less likely, are both associated with optimism bias in board level perception.

4.2 Pessimism bias

Pessimism bias is defined as the tendency to overestimate negative outcomes and perceive risks as more severe than they actually are (Snow et al., 2007). Sometimes the board sees threats as too close, which makes them overly negative or even hopeless. CISO#3 said, "After observing a peer organization fall victim to ransomware, a board member remarked: 'It's just a matter of time for us.'" Because the affected organization is familiar, the social distance was reduced and the board suddenly recognized their exposure to the same risk. Consequently, the risk becomes urgent and unavoidable.

Another CISO#10 noted: "Following the Log4j incident, they (board members) were prepared to terminate all new technology projects." In this scenario, reduced hypothetical distance made a general threat appear concrete, while reduced social distance led the board to perceive the risk as directly relevant to their organization. As a result, they reacted with immediate measures, even if those responses were not always proportionate.

CISO#5 mentioned, "We'll never be secure, no matter what we do." This shows how perceiving the threat as imminent (reduced temporal distance) and almost certain to occur (reduce hypothetical distance) can foster extreme pessimism, making any effort seem pointless.

In short, pessimism bias happens when the threat feels psychologically close, either socially, in time, or in likelihood. That closeness makes board members zoom in on the risk and lose sight of the broader context. It can lead to fear-based decisions, overreactions, or even a disengagement from longer-term security initiatives. From the perspective of CLT, pessimism bias arises because of reduced psychological distance leads boards to think in concrete terms, making immediate threats feel more pressing while pushing broader and longer-term considerations into the background.

4.3 Ambiguity bias

Ambiguity bias is defined as the tendency to avoid or undervalue options where information is conflicting, incomplete, or uncertain (Bhandari et al., 2008). In this context, such ambiguity is often represented by 'amber risks' positioned between the clear danger of red and the relative safety of green. Boards only react to well-defined threats and often avoid those they do not fully understand. CISO#7 observed: "The board shows a tendency to postpone the discussion of 'amber risks' time after time." Such procrastination increases the temporal distance, which allows the issue to remain vague and less urgent.

CISO#6 said: "If I can't reduce it to traffic-light colors, they push it to the side." This demonstrates how visual clarity can reduce hypothetical distance and make engagement more likely. Conversely, risks without such framing remain psychologically remote and are deprioritized. A third example came from CISO#9 who recalled: "They (board members) don't like grey areas. They want yes/no answers." Here, the absence of certainty increases hypothetical distance, when risks are presented in shades of gray, the board perceives them as not concrete enough to warrant attention.

In short, ambiguity bias arises when unclear or complex risks get ignored, not because they're unreal, but because they're too messy to evaluate. If something feels too abstract, the board avoids it. Boards prefer simple over nuanced interpretations, which can result in blind spots in how emerging threats are evaluated and addressed.

4.4 Confirmation bias

Confirmation bias is defined as the tendency to favor information that supports pre-existing beliefs or hypothesis while disregarding or undervaluing contradictory evidence (Snow et al., 2007). Boards do not only seek clarity, but they also prefer familiarity. CISO#7 noted: "They always ask: 'Is this GDPR-related?' If not, they switch off." Here perceived relevance is framed through compliance such that issues linked to GDPR are seen as close or urgent, whereas other risks feel distant and are overlooked.

CISO#9 observed: "They want to see the same phishing report every month, even if it's no longer relevant." Because phishing is familiar, it feels close and manageable. Even when actual risks have shifted, the board remains focused on familiarity that reduces hypothetical distance and provides a sense of control.

CISO#8 noted, "They only engage when incidents matching what they already worry about" If a threat does not connect with past experiences or existing concerns, it is construed as abstract or unrelatable, showing increased social- and hypothetical distance and therefore receives little attention.

In short, confirmation bias shows up when boards stick to the risks they already recognize. Risks outside this frame are perceived as distant or difficult to interpret. As a result, emerging threats can be overlooked, simply because they don't fit the mental checklist the board already holds.

5 Psychological Distance and the Amber Light

Based on the logic of CLT and the way psychological distance shapes optimism, pessimism, ambiguity, and confirmation bias, we can also better understand how traffic light reporting is interpreted in board contexts. In our interviews, all eleven CISOs confirmed that they use traffic light reporting as their primary way of communicating cybersecurity risk to boards. The amber indicator is particularly revealing, as it embodies ambiguity: unlike green (no issues) or red (critical risk), amber lacks a clear interpretation and leaves room for subjective judgement. This ambiguity means that responses can vary across individual boards members, depending on their experience, risk tolerance, or intuition. In this way, the amber

light is not merely a reporting mechanism but a mechanism through which the role of psychological distance and cognitive bias in decision-making becomes visible.

Building on this perspective, our interviews further reveal practices and rationales behind the use of traffic light reporting. CISOs emphasized its clarity, visual simplicity, and often efficiency in communicating complex issues, as well as its alignment with the board's preference for abstraction and simplification.

From a temporal perspective, several CISOs observed that boards tend to postpone the discussion of amber risks. As CISO#7 explained: "The board shows a tendency to postpone the discussion of amber risks time after time." CISO#6 mentioned that when traffic lights remain unchanged, always green, amber, or red, board members often ask: "What do I do to change that". Social distance plays a similar role in shaping how amber is perceived. CISOs emphasized that board members often ignore ambiguous risks until an incident affects a peer organization. CISO#11 noticed that after a DDoS attack, the board immediately asked, "Does this also apply to us?" CISO#11 uses high-profile cases such as "NotPetya" in Rotterdam to make risks feel closer: "Then they say: okay, that's our ecosystem, that could be us."

The hypothetical dimension also plays a crucial role in understanding amber. Several CISOs mentioned that green and red are straightforward, but amber causes discussion. At times, reports are presented in abstract or generalized terms, which may unintentionally increase psychological distance and reduce engagement. In other instances, CISOs deliberately add detail, specificity, or urgency to lower the construal level, thereby making the risk appear more applicable. This illustrates how communicative alternatives can actively raise or lower psychological distance, aligning message framing with intended board behavior. Notably, narratives and scenarios are also used by some CISOs to reduce hypothetical distance. By describing real-life incidents, sector-specific breaches, or near-miss events, they aim to decrease abstraction and increase perceived feasibility. CISO#8 explained that "If you focus on the amber light, I think that's where my experience as the CISO has to come into play, because I can't offload my risk register to the board". Spatial distance influences how boards perceive and sometimes downplay risks associated with third parties. As CISO#9 explained: "If it's amber because of a supplier, they'll say it is outside their scope." CISO#6 noted: "We are already preparing, but the boards perceive it as far away. Until it turns red, it stays abstract for them."

The reflection above aligns with Eling et al. (2021), who emphasize the role of risk analysis stage in restructuring ambiguity. By systematically assessing cyber risks as a combination of probability and impact, CISOs can translate "amber" signals into more concrete evaluations that boards can act upon. Taken together, these patterns show that the way CISOs report to boards reflects not only their strategic priorities but also an active management of psychological distance. By varying abstraction, detail, and narrative, they influence how risks are construed and ultimately, how decisions regarding cybersecurity are made. In summary, the present research suggests that 'amber' is not a neutral middle state but a psychological distance-dependent signal: psychologically distant amber tends to be interpreted as almost green, whereas psychologically close amber is treated as almost red. This dynamic character of amber has been largely overlooked in cyber risk reporting research to date.

6 Discussion, Contribution, and Future Research

This study has explored how psychological distance and construal levels shape the way board members interpret and act upon cybersecurity, based on insights from CISOs. By applying CLT as a lens, we show that cognitive biases regularly observed in the boardroom are not random flaws in judgement but rather predictable consequences of distance-driven mental framing.

The potential contribution lies in extending CLT into the domain of cybersecurity governance. Our initial findings show that psychological distance provides a systematic explanation for how boards construe cybersecurity risks and why certain biases emerge in a governance context. Our work positions psychological distance as a central mechanism structuring board-level decision-making.

A central paradox emerging from our findings is that both too much distance and too little distance can distort decision-making. Optimism bias emerges when threats feel far away, but pessimism bias arises when they feel uncomfortable close. This raises the question of whether the goal should be to minimize psychological distance or rather to balance it. CISOs may need to adjust the way they present risks, keeping reports high-level when the boards need to discuss strategy, but making them more concrete when action is required.

The findings in this paper showcase an important first step by demonstrating how CLT offers a structured explanation for biases in cyber risk reporting. These insights highlight that psychological distance is not just a background factor but a central mechanism that influences how board members interpret and act upon cybersecurity risks. Several limitations should be acknowledged when interpreting these findings. The study is based on a small convenience sample of eleven CISOs, limiting generalisability, and is skewed towards participants from the Netherlands and Belgium and predominantly large organizations. In addition, the reliance on single-informant self-reported data from CISOs may introduce selection and social desirability biases. Finally, the qualitative design is exploratory in nature and does not permit causal claims regarding the relationship between psychological distance and board-level decision-making.

Conceptually, our study extends work on cyber risk communication, particularly the "amber light" category, by showing that this middle category is not interpreted as neutral but rather shifts depending on how psychological distance is framed. When risks are communicated as *distant in time or as unlikely to occur*, amber tends to be perceived as not yet urgent (i.e., the interpretation moving toward the green light), whereas when risks feel closer or more personally relevant, amber can be perceived as more concerning (i.e., the interpretation moving toward the red light). This insight positions the amber light as a dynamic communication point where psychological distance framing shapes how boards construe risks and decide whether to act.

As the next step, we will conduct additional interviews with CISOs to further refine these propositions and explore additional aspects of CLT, such as desirability and feasibility. A later stage of the research will empirically test these propositions through an experiment that systematically manipulates psychological distance and construal levels. Building on our exploratory findings, the experiment will contrast situations in which the CISO presents risks in a high-level construal, abstract way (focusing on strategic relevance) versus a low-level construal, concrete way (emphasizing technical details). This design may reveal the tension we observed, i.e., boards typically operate at higher construal levels, while CISOs often frame risks more concretely. Just as CISOs can adjust psychological distance in their reports to influence how boards construe risks, the experiment will test how different framing in reporting strategies shift boards' construal levels and shape cybersecurity decisions. In doing so, we aim to clarify whether and how adjusting psychological

distance through adaptive communication between CISOs and boards is part of effective cybersecurity governance.

References

Armor, D. A., & Sackett, A. M. (2006). Accuracy, error, and bias in predictions for real versus hypothetical events. *Journal of Personality and Social Psychology, 91*(4), 583-600.

Barre, G. (2025). From Breakers to Builders: The Role of Bug Bounty Hunters in Strengthening Organizational Cybersecurity. *Information*, *16*(3), 209.

Barre, G., Huygh, T., Nguyen, D. K., & Nuijten, A. (2025). Towards understanding cognitive biases in cybersecurity governance. *Proc. 38th Bled eConference*, 737-744.

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security, 63*, 1-13.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review, 24*(1), 93-125.

Eyal, T., Liberman, N., Trope, Y., & Walther, E. (2004). The pros and cons of temporally near and distant action. *Journal of Personality and Social Psychology, 86*(6), 781-795.

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PloS one, 15*(5), 2-6.

Kahneman, D. (2011). Fast and slow thinking. *Allen Lane and Penguin Books, New York, 2*.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *Mis Quarterly, 38*(2), 457-467.

Legoux, R., Leger, P. M., Robert, J., & Boyer, M. (2014). Confirmation biases in the financial analysis of IT investments. *Journal of the Association for Information Systems, 15*(1), 33-52.

Liberman, N., Sagristano, M. D., & Trope, Y. (2002). The effect of temporal distance on level of mental construal. *Journal of Experimental Social Psychology, 38*(6), 523-534.

Medin, D. L., & Smith, E. E. (1984). Concepts and concept formation. *Annual Review of Psychology, 35*(1), 113-138.

Noh, H. H., Rim, H. B., & Lee, B. K. (2025). Risk preferences in decision-making: A construal level perspective. *Acta Psychologica, 252,* 2-4.

Rosch, E. (1975). Cognitive representations of semantic categories. *Journal of Experimental Psychology: General, 104*(3), 192-233.

Snow, A. P., Keil, M., & Wallace, L. (2007). The effects of optimistic and pessimistic biasing on software project status reporting. *Information & Management, 44*(2), 130-141.

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review, 117*(2), 440-463.

Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. European *Journal of Information Systems, 23*(2), 223-239.

Wakslak, C. J., Trope, Y., Liberman, N., & Alony, R. (2006). Seeing the forest when entry is unlikely: probability and the mental representation of events. *Journal of Experimental Psychology: General, 135*(4), 641-653.