RESEARCH IN PROGRESS

TOWARDS UNDERSTANDING COGNITIVE BIASES IN CYBERSECURITY GOVERNANCE

GULET BARRE, TIM HUYGH, DINH KHOI NGUYEN, ARNO NUIJTEN

Open University of the Netherlands, Faculty of Science, Limburg, the Netherlands
gulet.barre@ou.nl, tim.huygh@ou.nl, khoi.nguyen@ou.nl, arno.nuijten@ou.nl

Cognitive biases can influence the decision-making of board members and CISOs responsible for managing cyber risks. However, limited attention has been given to understanding how these biases affect cybersecurity governance, specifically in the communication of risks between CISOs and boards. This paper aims to address this gap by identifying cognitive biases and proposing how these biases influence communication and strategic decision-making in cybersecurity governance. By further examining their impact, we strive to uncover the mechanisms that contribute to underestimations or distortions in risk perception, which can compromise an organization's ability to respond effectively to cyber threats. This short paper provides three exemplary biases expected to influence communication and decision-making in cybersecurity governance. Following the initial results, we propose a series of interviews with CISOs to reveal the challenges they face when communicating cyber risks to boards, focusing on how biases influence the decisions regarding cybersecurity risks.

DOI
https://doi.org/10.18690/um.fov.4.2025.46

ISBN
978-961-286-998-4

Keywords:
cybersecurity governance, board decision-making, cognitive biases, risk communication, cyber threats

University of Maribor Press

1 Introduction

Despite cybersecurity being recognized as a critical component of corporate governance and something that should be on the radar of the board of directors (De Haes et al., 2020), many boards remain ill-equipped to fulfil their strategic responsibilities in managing cyber risks (Valentine, 2016). To be able to take responsibility for cyber risk in the boardroom and ask the right questions to the CISOs within the organization, thereby holding them accountable, adequate governance measures should be in place. This pertains to proper information about cyber risks coming from the organization and board composition and expertise to be able to make an appropriate assessment of cyber risks (Smaili et al., 2022).

Moreover, decision-making in the boardroom is inherently complex. Directors rely on mental shortcuts, known as heuristics, to simplify information processing. Although heuristics can expedite decision-making, they can frequently lead to systematic errors called cognitive biases (Berthet, 2022). Such biases can significantly influence the decision-making process, particularly in the context of cybersecurity governance (Vedadi & Warkentin 2020). In other words, any decision-making is subject to biases in how we process information and estimate risks.

While we identify six biases through a systematic literature review, this short paper discusses three exemplary cognitive biases that affect board-level decision-making in the context of cybersecurity governance. We subsequently aim to address the following research question: What specific biases influence boards and CISOs communication and interactions regarding cybersecurity? Particularly, we validate and expand these biases by conducting interviews with CISOs. By exploring how cognitive biases manifest in decision-making in cybersecurity governance, we aim to pinpoint which biases are most relevant in practice and under which scenarios the biases emerge.

Our intermediate results indicate that there is a fragmented understanding of cognitive biases within the domain of Information Systems (IS), and no literature to date investigates relevant biases in the context of cybersecurity governance. Therefore, our study contributes in the following ways. We outline a literature review of cognitive biases within leading IS literature, and rationalize the relevance of these biases in the context of cybersecurity governance. As such, we demonstrate cognitive

biases as a meaningful theoretical lens to understand board-level communication and decision-making around cybersecurity. Toward this contribution, this study validates the results with biases identified in broader board-level decision-making literature. We will also empirically investigate these findings through interviews with CISOs.

2 Scope of Literature Search and Procedure

Our search methodology aligns with the evolving academic discourse surrounding biases and their implications for risk assessment and decision-making in cybersecurity. We initiated our investigation by exploring core terms that encapsulate the essence of our study: 'bias' and 'risk.' These terms were selected for their broad applicability and relevance across a spectrum of studies pertaining to decision-making and judgment in organizational contexts. To ensure a comprehensive and academically robust foundation, we utilized the Senior Scholars' List of Premier Journals as a basis, combined with snowballing.

To ensure a focused and efficient selection process, we established a set of criteria for identifying papers that would be relevant to our study. Specifically, we sought publications where the terms related to biases appeared prominently in the title, keywords, or abstract. This step was essential to exclude articles that only tangentially mentioned bias without exploring it as a primary topic of investigation. The application of these criteria enabled us to refine our search and identify papers that specifically addressed the types of biases pertinent to our research. We looked at papers published between January 1992 and September 2023. The initial screening phase resulted in 120 papers. We then applied a snowballing technique (both backward and forward), using the same inclusion/exclusion criteria to identify additional relevant papers. Although there was an overlap among papers due to similar research focus, this overlap helped confirm the significance of key studies and increased the reliability of the examined papers. The papers were selected based on their apparent alignment with our research focus, demonstrating a range of biases. Each of these papers was subsequently subjected to a manual review process, wherein we examined their content to verify their relevance and depth of analysis on bias-related issues.

During the manual review, papers that did not sufficiently address or identify bias as a primary subject were excluded from further consideration. This step was crucial in ensuring that only papers with substantial discussions on bias, whether through theoretical analysis, empirical investigations, or methodological studies, were included in the final list for deeper examination. The review process facilitated the exclusion of papers that, while potentially informative, did not contribute directly to our objective of understanding biases within decision-making frameworks in the IS context.

Ultimately, the combination of database search, keyword filtering, and manual review enabled us to curate a robust and relevant set of 52 papers. We identify six biases, and provide discussions on three exemplary biases below.

3 Exemplary biases

3.1 Optimism - Pessimism bias

Literature from the field of IS typically characterizes optimism bias as an individual's general tendency to underestimate the probability of unfavorable outcomes (Legoux et al., 2014). The opposite of optimism bias is pessimism bias, which occurs when a manager reports a project is in a worse state than it actually is (Snow et al., 2007).

The primary mechanism that influences optimism bias is overconfidence. This phenomenon manifests in two primary ways: overreaction and underreaction in the market (Daniel et al., 1998). Overreaction occurs when investors attribute excessive significance to their information, causing stock prices to rise or fall excessively. Conversely, underreaction happens when investors underestimate or ignore new public information, resulting in delayed price adjustments. Overconfidence amplifies both behaviors, causing prices to deviate from the actual fundamentals of the market. According to Daniel et al. (1998), the trigger that elicits this reaction is private information signals. Specifically, investors receive new private information, such as analyst reports, which serves as a trigger for investor overconfidence (Hilary & Menzly, 2006). Consequently, this leads to stock prices being displaced from their intrinsic value based on inaccurate assessments (Odean,1998). In the context of cybersecurity, this can manifest when individuals receive new information, for example, a report indicating that their systems are due for new security audits. This

trigger may give decision-makers a misleading sense of security, making boards believe their defenses are stronger than they actually are. As a result, boards may overlook potential risks and believe that they are fully protected, which can leave their organization vulnerable to cybersecurity threats.

A second mechanism is risk perception, which is defined as the subjective evaluation of the probability and potential severity of a risk among individuals and groups. Risk perception in cybersecurity mostly stems from subjective evaluations of the likelihood of a cyberattack (Eling et al., 2021). An example is, after hearing of a significant ransomware attack in the industry, board members may overestimate the probability of a similar attack within their organization.

3.2 Herding bias

The IS literature defines herding as an individual's propensity to conform to the behavior of preceding peers. This mechanism typically emerges in environments characterized by uncertainty. When individuals lack confidence in their knowledge, they are more inclined to follow others (Baddeley, 2013). Observing the actions of peers, they assume that the majority possesses superior information (Baddeley, 2013). The rationale is that if a larger number of people believe something, it may be perceived as more accurate (Bikhchandani et al.,1992). This trigger creates a process known as informational cascades, which occur when an individual observes the actions of predecessors and adopts their decision without considering their own judgment (Wang & Greiner, 2010).

Herding is observable in managerial decision-making. According to Kaufman and Li (2003), IT managers are known to follow crowds when making decisions regarding IT investments. This tendency to herd shows that managers may prioritize conformity over independent risk assessments, as they believe others' decisions are based on relevant information (Zhou & Lai, 2009). Therefore, managers may focus on supporting their choices with perceived consent rather than making decisions based purely on their own risk preferences (Vedadi & Warkentin, 2020). This behavior is also evident at the board level, where boards may often make decisions about cyber risk in response to external pressures, rather than basing it on their own risk appetite (Benaroch & Chernobai, 2017) For example, boards may respond to high-profile incidents such as data breaches or ransomware attacks by investing in

new security tools, primarily to emulate peer organizations, rather than selecting measures aligned with their own specific cyber risk profile (Kwon & Johnson, 2014).

As individuals' experiences can offer significant insights, it is vital for IT managers to create an environment that values individual insights, thus providing room for personal experience in decision-making. Neglecting such an environment increases the risk of errors due to herding. In the cybersecurity context, past research shows that managers upscaled their organization's security by the information they received about the security behavior of others (Barlow et al., 2018; Vedadi & Warkentin, 2020).

4 Discussion and Prospective Research Pathway

This study ultimately seeks to advance our understanding of how cognitive biases can influence the decision-making process in the context of cybersecurity governance. Our preliminary findings highlight a fragmented understanding of cognitive biases within the IS domain, with no prior research specifically addressing cognitive biases in the context of cybersecurity governance. This study bridges this gap in the following ways. First, we present a comprehensive literature review of cognitive biases within leading IS literature and rationalize their relevance to cybersecurity governance. Second, we demonstrate cognitive biases as a meaningful theoretical lens to understand board-level communication and decision-making on cybersecurity issues.

To these ends, we aim to integrate research on cognitive biases and board-level decision-making in the context of cybersecurity. By focusing on the specific impact of these biases on critical cybersecurity areas, this study lays the foundation for developing a comprehensive bias-aware approach to improve decision-making in cybersecurity governance. The overall goal of this research is to provide a set of theory-driven guidelines for board members and CISOs to make better decisions by recognizing and mitigating these biases.

The preliminary results presented in this paper contribute to the understanding of how cognitive biases affect cybersecurity governance decision-making. These insights foresee an important first step toward the ambition of this research, which

is to improve the decision-making of board members and CISOs, by integrating awareness of psychological influences into the strategic management of cyber risks.

The next phase of this study involves the extension and empirical validation of our preliminary results. Particularly, we refine these results through cross-referencing biases identified in broader (non-IS) board-level decision-making literature and subsequently empirically validate them via semi-structured interviews with CISOs. Regarding the interviews, we aim at indirectly asking CISOs about challenges and pinpointing these challenges to different identified biases. This strategy ensures that CISOs do not simply deny certain biases, which could potentially hinder obtaining interesting insights (Merendino et al., 2018). This validation phase is essential to fulfilling our overall objective: to help boards and CISOs make better-informed decisions by considering psychological factors (biases) that may influence their judgment in the context of cybersecurity.

References

Baddeley, M. (2013). Herding, social influence and expert opinion. *Journal of Economic Methodology, 20*(1), 35-44.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems, 19*(8), 3.

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value destruction, and board-level IT governance changes. *MIS Quarterly, 41*(3), 729-A6.

Berthet, V. (2022). The impact of cognitive biases on professionals' decision-making: A review of four occupational areas. *Frontiers in Psychology, 12*, 802439.

Bikhchandani, S., Hirshleifer, D., & Welch, I. (1992). A theory of fads, fashion, custom, and cultural change as informational cascades. *Journal of Political Economy, 100*(5), 992-1026.

Daniel, K., Hirshleifer, D., & Subrahmanyam, A. (1998). Investor psychology and security market under-and overreactions. *The Journal of Finance, 53*(6), 1839-1885.

De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., De Haes, S., Van Grembergen, W., ... & Huygh, T. (2020). Enterprise Governance of IT, alignment, and value. *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, 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.

French, A. M., Storey, V. C., & Wallace, L. (2023). The impact of cognitive biases on the believability of fake news. *European Journal of Information Systems*, 1-22.

Hilary, G., & Menzly, L. (2006). Does past success lead analysts to become overconfident?. *Management Science, 52*(4), 489-500.

Jiang, Y., Ho, Y. C., Yan, X., & Tan, Y. (2022). What's in a "username"? The effect of perceived anonymity on herding in crowdfunding. *Information Systems Research, 33*(1), 1-17.

Kaufmann, C., & Kock, A. (2023). The performance effects of optimistic and pessimistic project status reporting behavior. *International Journal of Project Management, 41*(7), 102514.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly, 38*(2), 451-A3.

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), 1.

Merendino, A., Dibb, S., Meadows, M., Quinn, L., Wilson, D., Simkin, L., & Canhoto, A. (2018). Big data, big decisions: The impact of big data on board level decision-making. *Journal of Business Research, 93*, 67-78.

Odean, T. (1998). Volume, volatility, price, and profit when all traders are above average. *The Journal of Finance, 53*(6), 1887-1934.

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance, 27*(4), 1049-1071.

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.

Valentine, E. L. (2016). *Enterprise technology governance: New information and technology core competencies for boards of directors* (Doctoral dissertation, Queensland University of Technology).

Vedadi, A., & Warkentin, M. (2020). Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. *Journal of the Association for Information Systems, 21*(2), 3.

Vlek, C. A. (1996). A multi-level, multi-stage and multi-attribute perspective on risk assessment, decision-making and risk control. *Risk Decision and Policy, 1*(1), 9-31.

Walden, E. A., & Browne, G. J. (2009). Sequential adoption theory: a theory for understanding herding behavior in early adoption of novel technologies. *Journal of the Association for Information Systems, 10*(1), 1.

Wang, H., & Greiner, M. (2010). Herding behavior in the stock market: Evidence from stock trading volume data of Chinese stock market. *Journal of Empirical Finance, 17*(3), 483-494.

Zhou, R. T., & Lai, R. N. (2009). Herding and information based trading. *Journal of Empirical Finance, 16*(3), 388-393.

Zou, H., Sun, H., & Fang, Y. (2023). Satisfaction to stay, regret to switch: understanding post-adoption regret in choosing competing technologies when herding. *Information Systems Research, 34*(4), 1455-1475.