International Business and Global Economy 2023/2024, no. 42, pp. 49–58

Edited by the Institute of International Business, University of Gdańsk
ISSN 2300-6102
e-ISSN 2353-9496 https://doi.org/10.26881/ibage.2023.42.04

Marc Wilczek
University of Gdańsk

Exploring the potential of behavioural economics in cyber-security – development of a conceptual framework

In recent years, the field of cyber-security has encountered unprecedented challenges due to the rapidly evolving nature of cyber-threats. Traditional cyber-security approaches often prioritize technical solutions and infrastructure, neglecting the critical role of human decision-making in cyber defence strategies. This paper delves into the intricate realm of cognitive biases within the cyber-security domain, investigating their profound influence on decision-making processes and organizational resilience from a behavioural economics perspective. Scholars have identified a multitude of biases, many of which directly impede actions and decisions in cyber-security. The paper addresses this gap in the literature by proposing a systematic and mixed research approach, which includes qualitative research followed by an empirical study. Through an examination of various biases and their implications, this research aims to illuminate the cognitive vulnerabilities inherent in cyber security and suggests strategies to mitigate their impact and reduce economic damage. Additionally, the study endeavours to narrow down the long list of biases and heuristics to the most prevalent ones through interviews, facilitating a more focused approach during the empirical study.

Keywords: cyber-risk, cyber-security, cybercrime, decision-making, cognitive biases

JEL classification: D81, D83, G3

Introduction

In the era of digital transformation, organizations globally are increasingly reliant on the Internet for their operations. This reliance extends to crucial aspects such as revenues, profits, reputation and supply chains, all which hinge upon the availability and integrity of IT networks and systems [Singh, Bakar, 2019]. However, this interconnectedness also exposes organizations to the looming threat of cybercrime, a menace that has witnessed exponential growth in recent years

[Brar, Kumar, 2018]. Within a more digitalized world, the prevalence of cognitive flaws presents a significant challenge, undermining the efficacy and security of commerce and economic prosperity. Despite all technical advances, the efficacy of cyber-risk management is significantly influenced by human actions and decisions [Frank, 2020]. With the growing amount of time people dedicate to online activities, their exposure to potential cyber-risks and the chances of being targeted by cybercriminals increase significantly [Leukfeldt, Yar, 2016]. However, there is a significant lack of research investigating biases and heuristics related to cyber issues, particularly in regard to subject matter experts responsible for implementing necessary safeguards [Alnifie, Kim, 2023; Ceric, Holland, 2019].

The urgency of addressing cognitive flaws within this context is emphasized by the economic consequences of cybercrime. With damages surpassing 1 trillion USD in 2020 alone [Cremer et al., 2022], cybercrime poses a significant risk to global economies, civil infrastructure and societies [Konradt et al., 2016]. The surge in cybercrime has been further accelerated by the COVID-19 pandemic, as well as the increasing trend towards remote working and heightened activity in the cyberspace [Duong et al., 2022]. Failing to mitigate cognitive biases not only puts organizational stability and reputation at stake but also exposes the potential for substantial financial losses in an increasingly digitalized world [Farahbod et al., 2020; Jalali et al., 2019]. Ultimately, this trend leads to the proliferation of externalities, further exacerbating the impact of cybercrime. Understanding and mitigating cognitive flaws within the cyber-context are crucial for navigating the complexities of the digital landscape effectively. Therefore, it is recommended to adopt a comprehensive research approach that combines qualitative and quantitative methods to explore cognitive biases in cyber-security. This approach entails gathering qualitative insights through expert interviews to identify and prioritize biases, followed by a validation study using a standardized questionnaire. By integrating both approaches, this research aims to provide valuable insights to improve decision-making in cyber-security. Collaboration among stakeholders across academia, industry, and government is paramount to prioritize research efforts aimed at addressing cognitive biases in the cyber-context, ultimately contributing to a safer and more secure cyberspace.

1. Definition of cognitive biases and heuristics

Cognitive biases and heuristics, otherwise known as judgmental flaws, represent consistent deviations from rationality and objective reality in the processes of judgment and decision-making. These deviations challenge the traditional economic assumption that humans are rational actors who always seek to maximize their utility. Notable studies, such as those conducted by Kahneman and Tversky [1974],

Tversky and Kahneman [1974], Kahneman and Tversky [1979], Thaler [1980], Tversky and Kahneman [1981] and Weinstein [1980], have brought to light these systematic deviations, emphasizing the constraints of human rationality across different scenarios. These biases stem from a variety of cognitive mechanisms, encompassing perception, memory and reasoning, and significantly impact human behaviour.

In the cyber-context, cognitive flaws manifest in nuanced ways, shaping individuals' interactions and beliefs, and often leading to misguided decisions [Alanazi et al., 2022]. Confirmation bias, for instance, predisposes individuals to seek out information that confirms their existing beliefs while disregarding contradictory evidence. Similarly, the availability heuristic leads individuals to overestimate the prevalence of information readily available in memory, often resulting in skewed perceptions and decisions. These biases can significantly impact decision-making processes within the cyber-security domain, where accurate assessments of risks and vulnerabilities are critical. Overreliance on intuitive judgments or cognitive shortcuts may lead to suboptimal outcomes, leaving organizations vulnerable to a growing number of cyber-threats. Recognizing and understanding these cognitive biases are essential for developing effective strategies to mitigate cyber-risks. By acknowledging the cognitive processes that influence decision-making, stakeholders can implement targeted interventions to minimize the impact of biases and enhance cyber-security posture.

In summary, cognitive biases and heuristics represent systematic deviations from rationality in judgment and decision-making processes. Within the cyber-context, these biases can have significant implications for organizational cyber-security, highlighting the importance of recognizing and addressing them proactively.

2. Manifestation in the cyber-context

In the cyber-context, cognitive flaws present a multifaceted challenge, influencing decision-making processes and cyber-security measures. The commonality among all of these biases is their tendency to mislead decision-makers and result in heightened risk and inefficient allocation of resources. As the world continues to shift towards digitalization, this issue is becoming a growing concern. Some examples of these judgmental flaws are further contextualized in Table 1.

While these are just some examples, understanding these cognitive flaws is critical for developing effective cyber-security strategies. Scholars have meanwhile identified over 150 biases [Brooks et al., 2020], with 87 directly impeding cyber-security actions [Johnson et al., 2020]. Recognizing these biases is vital for mitigating cyber-risks and enhancing organizational resilience. However, research in this area is still scarce, warranting further inquiry.

Table 1. Cognitive biases in the cyber-security context

Bias	Implication
availability heuristic	Recent incidents like data breaches serve as a catalyst for taking measures to enhance cyber-security. However, in the absence of up-to-date news and events, the importance of cyber-security may be diminished and not given the necessary priority it deserves.
confirmation bias	Individuals process information in a way that aligns with their existing defence strategy. Crucial information or data may be misinterpreted, leading to security breaches or ineffective resilience.
optimism bias	Individuals fail to accurately assess the likelihood of negative events occurring, leading them to underestimate the risk of cyber-threats and mistakenly believe that they will not encounter a cyber-attack.
anchoring bias	Decision-makers may anchor their budget allocations on historical spending patterns and events. Especially the absence of cyber-attacks may lead to insufficient future investments.
loss aversion	Although loss aversion promotes carefulness, it can also hinder creativity and proactive risk mitigation efforts. It may fosters resistance to change and contributes to a status quo bias, where individuals are more inclined to preserve the current set of tools and resist embracing new cyber-security strategies, even in the face of evolving threat landscapes.
overconfidence bias	Individuals overestimate their ability to detect and respond to cyber-threats effectively. This unwarranted confidence can lead to complacency, leaving organizations vulnerable to sophisticated attacks.

Source: Own elaboration.

In conclusion, cognitive biases significantly impact decision-making and efforts across the cyber-domain [Alsharida et al., 2023]. By addressing biases like overconfidence, optimism, anchoring, confirmation bias, loss aversion and status quo bias, organizations can strengthen their cyber-resilience and better protect against evolving threats. Collaboration between academia, industry and government is essential to drive further research and develop actionable insights for addressing cognitive flaws undermining cyber-resilience.

3. Proliferation of cybercrime and examples

The rise of cybercrime, driven by technological advancements and the advent of cybercrime-as-a-service (CaaS), has created new opportunities for individuals to partake in unlawful endeavours [Huang, Madnick, 2017]. Moreover, it acts as a catalyst, amplifying the frequency of cyber-attacks and contributing to their escalating numbers. Criminal marketplaces, flourishing on the dark web, offer a wide range of illicit goods and services, including stolen credentials, malware, and hacking tools, enabling individuals to engage in cybercrime with relative ease [Europol, 2023; Huang et al., 2018].

One notable consequence of this CaaS proliferation is the emergence of ransomware attacks targeting organizations worldwide. These attacks, facilitated by the availability of ransomware kits and CaaS platforms on the dark web, allow even individuals with limited technical expertise to launch sophisticated cyber-attacks for financial gain [Huang, Madnick, 2017]. By exploiting cognitive biases such as urgency and fear of loss, ransomware operators manipulate victims into paying exorbitant ransoms to regain access to their compromised data.

One such example is the cyber-attack on Maersk, which serves as a stark reminder of the serious repercussions of cyber-security incidents. As one of the largest global shipping companies, Maersk fell victim to the NotPetya ransomware attack, causing widespread disruptions to its operations worldwide. The attack targeted essential systems, leading to a complete network shutdown over multiple weeks. The financial impact of the attack was significant, with losses exceeding 300 million USD [Greenberg, 2018]. It also put a dent on Maersk's reputation, undermining customer trust in its data protection capabilities. The rapid spread of the malware was akin to a wildfire, impacting a significant number of organizations spanning across 60 countries within just a matter of days. According to reports from the US White House, the total damage caused by the NotPetya malware campaign is projected to exceed 10 billion USD [Wolff, 2022].

Another compelling case study directly linked to human error is Capital One, the eighth largest bank in the United Sates. In this instance, a misconfiguration in their AWS Cloud allowed a threat actor to gain access to confidential data belonging to around 100 million American citizens and 6 million Canadian citizens [Khan et al., 2022]. Without factoring in any associated expenses required to restore their operations, the bank faced a regulatory fine of 80 million USD. Furthermore, they also reached an agreement to compensate the affected customers with a settlement amounting to 190 million USD due to the violation of privacy [Avery, 2022]. This incident serves as a testament of the consequences that can arise from human error in mission-critical systems.

These examples underscore the critical need for organizations to recognize and mitigate cognitive biases in cyber-security practices. Despite having cyber-security measures in place, these cases illustrate how companies may underestimate cyber-threats and the occurrence of hazardous events and put measures in place that ultimately prove to be inadequate. It is crucial to examine why these biases occur and why they persist, prompting organizations to scrutinize the matter more closely to reduce their risk exposure. By fostering a culture of inquiry and introspection, organizations can empower their workforce to recognize and address these biases more effectively. This thorough examination of the underlying factors contributing to cognitive biases is essential for organizations to strengthen their cyber-security defences and adapt to the surging cyber-threat landscape.

In summary, the proliferation of cybercrime, facilitated by advancements in technology and the availability of criminal marketplaces on the dark web, underscores the critical need for organizations to address cognitive biases in their cyber-security strategies. By recognizing the influence of cognitive biases and implementing measures to mitigate their impact, organizations can better protect themselves against evolving cyber-threats and safeguard their digital assets, reputation, and stakeholders' trust.

4. Implications and importance of further study

Understanding the prevalence of cognitive flaws within the cyber-context is crucial for several reasons. Firstly, it allows organizations to develop more effective strategies for mitigating cyber-risks and enhancing their overall resilience. By recognizing the cognitive biases that impede decision-making processes, stakeholders can implement targeted interventions to minimize their impact and improve their cyber-security posture.

Secondly, further study in this area is essential for advancing the field of cyber-security and risk management. By delving deeper into the underlying mechanisms of cognitive biases and their manifestation in the cyber-context, researchers can uncover new insights and develop innovative solutions for addressing these challenges. This knowledge can inform the development of more robust cyber-security practices, leading to better protection against cyber-threats and minimizing economic damage.

Furthermore, the implications of cognitive flaws extend beyond individual organizations to society. As cyber-attacks continue to pose significant threats to national security, economic stability and public safety, understanding and addressing cognitive biases are critical for safeguarding collective interests. By fostering greater awareness and collaboration among stakeholders, further study in this area can contribute to a safer and more secure digital environment for all.

In summary, the importance of further study into the prevalence of cognitive flaws within the cyber-context cannot be overstated. By uncovering new insights and developing targeted interventions, researchers can empower organizations to navigate the complexities of the digital landscape more effectively and mitigate the ever-evolving cyber-threat landscape.

In the exploration of cognitive flaws within the cyber-context and the development of actionable insights, the following research approach is recommended. Through in-depth interviews with subject matter experts in the cyber-security domain, insights will be gathered to identify and prioritize prevalent cognitive biases. Engaging directly with experts immersed in the complexities of cyber-threats

aims to shed light on biases significantly impacting decision-making processes. By employing qualitative research methods, such as a combination of deductive and inductive reasoning, data collected from interviews will be analysed. This analysis aims to condense the extensive list of biases into a concise selection of the most prevalent ones. The systematic categorization and synthesis of insights will uncover common themes and patterns characterizing cognitive biases in the cyber-context. Next, a structured validation study based on a standardized questionnaire will be designed and implemented to cross-validate findings from expert interviews. The broader survey of subject matter experts using this method will facilitate the assessment and impact of identified cognitive biases, enabling the discovery of potential correlations and trends across a much larger data sample.

This iterative approach embraced throughout the research process will allow for continual refinement, and updating of recommendations. Informed by insights gathered from the synthesis of expert interviews and empirical validation, actionable recommendations will be formulated. These recommendations may include training initiatives, organizational policies and procedures, and the design of decision-support tools. The objective is to bolster cognitive resilience and enhance the quality of decision-making in the realm of cyber-security.

Conclusions

The prevalence of cognitive flaws within the cyber-context poses a formidable challenge, exerting profound impacts on decision-making processes, cyber-security measures, and the overall resilience of organizations. By conducting thorough interviews with subject matter experts and carrying out empirical validation studies, researchers can explore the complex network of cognitive biases that exist within the field of cyber-security. This approach allows them to gain valuable insights into the extensive implications of these biases.

Drawing from theoretical perspectives in cognitive psychology and behavioural economics, this research sheds light on the underlying mechanisms driving cognitive biases in the cyber-context. The insights gleaned from studies such as those conducted by Kahneman and Tversky provide valuable frameworks for understanding how individuals process information and make decisions in uncertain and high-pressure cyber-security environments. Moreover, the findings from behavioural economics, as exemplified by the research on overconfidence, optimism, anchoring, confirmation bias, loss aversion, and status quo bias, underscore the irrational behaviours and biases that impede decision-making processes in cyber-security contexts.

By integrating these theoretical perspectives into the analysis of cognitive biases in the cyber-context, researchers can provide a more comprehensive understanding of how these biases manifest and their implications for cyber-security measures. This enriched theoretical foundation not only informs the identification and prioritization of cognitive biases but also facilitates the development of targeted interventions and mitigation strategies.

By distilling the extensive array of biases into a concise yet comprehensive shortlist, and subsequently crafting actionable recommendations for mitigating their detrimental effects, organizations can fortify their cognitive resilience. Armed with these insights, decision-makers can navigate the complex landscape of cyber-threats with greater acumen and foresight, making well-informed decisions even in the face of a rapidly evolving threat landscape.

As the world increasingly embraces digitalization, the susceptibility to cyber-risk escalates exponentially. Therefore, it becomes imperative for stakeholders spanning academia, industry, and government sectors to foster collaboration and channel resources toward prioritizing research endeavours aimed at unravelling the intricate workings of cognitive biases. Addressing these biases head-on is paramount, as they have the potential to undermine decision-making processes, leading to suboptimal outcomes and heightened vulnerability to cyber-threats.

References

Alanazi M., Freeman M., Tootell H., 2022, *Exploring the factors that influence the cybersecurity behaviors of young adults*, Computers in Human Behavior, no. 136, doi.org/https://doi.org/10.1016/j.chb.2022.107376.

Alnifie K.M., Kim C., 2023, *Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta analysis*, Journal of Information Security, no. 2, doi.org/10.4236/JIS.2023.142007.

Alsharida R.A., Al-Rimy B.A.S., Al-Emran M., Zainal A., 2023, *A systematic review of multi-perspectives on human cybersecurity behavior*, Technology in Society, no. 73, doi.org/https://doi.org/10.1016/j.techsoc.2023.102258.

Avery D., 2022, *Capital one $190 million data breach settlement: Today is the last day to claim money*, CNET, cnet.com/personal-finance/capital-one-190-million-data-breach-settlement--today-is-deadline-to-file-claim [access: 12.10.2023].

Brar H.S., Kumar G., 2018, *Cybercrimes: A proposed taxonomy and challenges*, Journal of Computer Networks and Communications, doi.org/10.1155/2018/1798659.

Brooks B., Curnin S., Owen C., Bearman C., 2020, *Managing cognitive biases during disaster response: The development of an aide memoire*, Cognition, Technology & Work, no. 22, doi.org/10.1007/s10111-019-00564-5.

Ceric A., Holland P., 2019, *The role of cognitive biases in anticipating and responding to cyberattacks*, Information Technology and People, no. 1, doi.org/10.1108/ITP-11-2017-0390/FULL/XML.

Cremer F., Sheehan B., Fortmann M., Kia A.N., Mullins M., Murphy F., Materne S., 2022, *Cyber risk and cybersecurity: A systematic review of data availability*, The Geneva Papers on Risk and Insurance – Issues and Practice, no. 3, doi.org/10.1057/s41288-022-00266-6.

Duong A.A., Maurushat A., Bello A., 2022, *Working from home users at risk of COVID-19 ransomware attacks*, Cybersecurity and Cognitive Science, doi.org/10.1016/B978-0-323-90570-1.00001-2.

Europol, 2023, *Cyber-attacks: The apex of crime-as-a-service (IOCTA 2023)*, europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023#downloads [access: 24.11.2024].

Farahbod K., Shayo C., Varzandeh J., 2020, *Cybersecurity indices and cybercrime annual loss and economic impacts*, Journal of Business and Behavioral Sciences, no. 1.

Frank M., 2020, *Using calibration to help overcome information security overconfidence* [in:] *Proceedings of the 41st International Conference on Information Systems, ICIS 2020, Making Digital Inclusive: Blending the Locak and the Global, Hyderabad, India, December 13–16, 2020*, eds. J.F. George, S. Paul, R. De', E. Karahanna, S. Sarker, G. Oestreicher-Singer, Association For Information Systems.

Greenberg A., 2018, *The untold story of NotPetya, the most devastating cyberattack in history*, Wired, wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world [access: 4.12.2023].

Huang K., Madnick M.S.S., 2017, *Cybercrime-as-a-service: Identifying control points to disrupt*, Working Paper CISL# 2017-17, web.mit.edu/smadnick/www/wp/2017-17.pdf [access: 24.11.2024].

Huang K., Siegel M., Madnick S., 2018, *Systematically understanding the cyber attack business: A survey*, ACM Computer Surveys, no. 4, doi.org/10.1145/3199674.

Jalali M.S., Siegel M., Madnick S., 2019, *Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment*, The Journal of Strategic Information Systems, no. 1, doi.org/10.1016/j.jsis.2018.09.003.

Johnson C.K., Gutzwiller R.S., Ferguson-Walter K.J., Fugate S.J., 2020, *A cyber-relevant table of decision making biases and their definitions*, doi.org/10.13140/RG.2.2.14891.87846/1.

Kahneman D., Tversky A., 1974, *Subjective probability: A judgment of representativeness* [in:] *The concept of probability in psychological experiments*, ed. C.-A.S. Staël Von Holstein, Springer, Dordrecht.

Kahneman D., Tversky A., 1979, *Prospect theory: An analysis of decision under risk*, Econometrica, no. 2, doi.org/10.2307/1914185.

Khan S., Kabanov I., Hua Y., Madnick S., 2022, *A systematic analysis of the capital one data breach: Critical lessons learned*, ACM Transactions on Privacy and Security, no. 1, doi.org/10.1145/3546068.

Konradt C., Schilling A., Werners B., 2016, *Phishing: An economic analysis of cybercrime perpetrators*, Computers & Security, no. 58, doi.org/10.1016/J.COSE.2015.12.001.

Leukfeldt E.R., Yar M., 2016, *Applying routine activity theory to cybercrime: A theoretical and empirical analysis*, Deviant Behavior, no. 3, doi.org/10.1080/01639625.2015.1012409.

Singh M.M., Bakar A.A., 2019, *A systemic cybercrime stakeholders architectural model*, Procedia Computer Science, no. 161, doi.org/10.1016/J.PROCS.2019.11.227.

Thaler R.H., 1980, *Toward a positive theory of consumer choice*, Journal of Economic Behavior & Organization, no. 1, doi.org/10.1016/0167-2681(80)90051-7.

Tversky A., Kahneman D., 1974, *Judgment under uncertainty: Heuristics and biases*, Science, no. 185.

Tversky A., Kahneman D., 1981, *The framing of decisions and the psychology of choice*, Science, no. 211, doi.org/10.1126/SCIENCE.7455683.

Weinstein N.D., 1980, *Unrealistic optimism about future life events*, Journal of Personality and Social Psychology, no. 5, doi.org/10.1037/0022-3514.39.5.806.

Wolff J., 2022, *Insurers must rethink handling of cyber attacks on states*, Financial Times, ft.com/content/aa147054-ec14-4a75-a183-bee345319948 [access: 4.12.2023].

M. Wilczek (✉) m.wilczek.720@studms.ug.edu.pl