4-1-2022

The Impact of Choice Overload on Decision Deferral in Cybersecurity

Cristian Alecse
University of Central Florida, cristian.alecse@ucf.edu

THE IMPACT OF CHOICE OVERLOAD ON DECISION DEFERRAL IN CYBERSECURITY

Cristian Alecse
University of Central Florida
cristian.alecse@ucf.edu

ABSTRACT

Since a large area of cybersecurity research is technically centered but most cyber incidents are human enabled (Nobles, 2018), a shift in focus towards behavioral issues is imperative to improve the understanding of these problems. Research in behavioral economics shows that cognitive biases can impact the decision-making process. For example, a seminal study conducted by Iyengar and Lepper (2000) reveals that a large array of product options attracted customers to browse, but fewer choices got them to buy. Similar research shows that when presented with a large array of options, customers tend to defer decisions, search for alternatives, or even opt not to choose. Choice overload bias describes how individuals get overwhelmed when presented with a large number of options to choose from. This study translates extant behavioral economics based research on choice overload from various disciplines (e.g., business, public administration, medical science, sociology) and explores its impact on cybersecurity.

Keywords

Behavioral cybersecurity, cognitive bias, choice overload, decision deferral

INTRODUCTION

The increasing number of cyber-attacks, data breaches, and ransomware attacks registered by organizations worldwide is largely the result of human error, with research showing that 95% of the cyber incidents are human enabled (Nobles, 2018). As the complexity of technology and information systems continuously increases, the human component becomes ever more predisposed to cybersecurity errors (Alavi et al., 2016). Nevertheless, the existing information security policies and plans created to prevent cybersecurity incidents refer almost exclusively to technology-related measures, with very little account for human behavior (Schultz, 2005). Likewise, the massive multi-billion-dollar investments in technological solutions meant to improve cybersecurity defense in organizations are largely disproportionate compared with the relatively small amounts allocated to mitigate human-related security issues (Metalidou et al., 2014). This approach is generally aligned with the neoclassical (standard) economics model of the preference-maximizing human behavior that looks at humans as rational-agents who have perfect self-control and make only rational choices when provided with adequate information (Kahneman, 2011). As consequence, the information security frameworks adopted by organizations are largely including humans as merely cybersecurity training and education beneficiaries (Cano, 2019), in the idea that providing them with optimal information combined with their innate unbounded rationality will be enough to ensure a good level of information security.

The development of the behavioral model of economics provides an alternative approach to the rational-agent theory by taking into consideration the effects of psychological factors on human decisions in an attempt to explain why people are often deviating from the rational-choice model (Thaler & Sunstein, 2021). Accepting humans as bounded-rationality agents allows us to probe why people are not always making the "rational" or "optimal" decisions, even in the conditions when they have a direct benefit to do it (Klaes & Sent, 2005) and facilitate ways to introduce new risk-management frameworks to prevent or correct irrational behavior occurrence that negatively impacts information security.

Despite the previous recognition of the importance of human behavior impact on cybersecurity and the early calls for increasing the research efforts in this area (Schultz, 2005), recent comprehensive analyses of the current research in the field continue to emphasize the need for more interdisciplinary approach that includes human behavior as a factor of influence in the security of computerized information systems (Lahcen, et. al, 2020). This study translates the findings of extant research in behavioral economics, to areas of cybersecurity and focuses on the potential impact of choice overload in the information systems security area by testing if (1) an extensive array of choices can lead to decision deferral with a negative impact on cybersecurity and if (2) decision task difficulty can moderate this relation.

BEHAVIORAL CYBERSECURITY

With the rapid development, extended accessibility and mobility of computers, and increased access to internet connectivity, the utilization of computerized information systems became common for millions of organizations of all types and sizes

worldwide. Consequently, the steep surge in information security breaches caused by human-related errors resulted in negative political, economic, and social consequences (Gandhi, et al., 2011), spurring a need for scientific exploration of the behavioral factors affecting the human-machine interaction. Although starting with the beginning of the 2010s the research community identified humans as the weakest link in cyberspace and recognized the critical role of the human-centered approach (Wiederhold, 2014), recent reviews of the literature on behavioral aspects of cybersecurity (Nobles, 2018; Lahcen, et. al, 2020) confirm that we are still in the incipient stage of the exploration in this area. One way to accelerate the knowledge development in the behavioral cybersecurity field can be the adaptation, translation, and assimilation of existent research from other scientific fields.

CHOICE IN BEHAVIORAL ECONOMICS

The neoclassical (standard) economics is based on a mathematical model of decision-making implying a fully rational process of the entire available information in order to identify the optimal choice. In contrast, behavioral economics combines elements of economics and psychology and embraces a bounded rationality approach, involving the use of heuristics and accepting the existence of cognitive biases to better understand human behavior. The behavioral economics approach is constructed on the premise that human behavior often deviates in predictable ways from making rational choices even when information abounds and enables processes that can enhance human decision-making (Lyons & Kass-Hanna, 2021).

The dual-system approach to decision making

Research revealed that humans use a dual process in making decisions through a combination of two systems (Kahneman, 2011). System 1, fast and automatic, is used to make decisions with a minimal cognitive effort involved, by using impressions, intuition, or pattern recognition (heuristics). System 2, slower and strenuous, is involving an elevated level of cognitive load employed to make calculated, informed decisions and choices by taking into account multiple data and options (analytical thinking). Heuristics are mental shortcuts that reduce cognitive load by utilizing rules-of-thumb to make rapid decisions. The dual-process theory indicates that the use of heuristics in the System 1 type of decision-making process leads to biases in how information is processed (Tversky & Kahneman, 1974). This can result in irrational behavior and erroneous choices (Gigerenzer & Selten, 2002). A cognitive bias is a subconscious systematic thinking error that occurs when individuals use their subjective perceptions of the world to process and interpret the information and frequently prevent them from making optimal decisions (Ariely, 2009). Individuals have no control over when and in what way System 1 operates, but they can intentionally choose to engage System 2 to reconsider the outputs from System 1.

Choice architecture

Choice architecture describes how different presentations of choices can influence individuals' decision-making and creates premises for using the presentation design as a tool in directing human decisions. For example, some of the choice architecture "tools" involve the use of default choices, complex choices structuring, creating incentives for taking decisions, or limiting the number of choices presented for decision. Behavioral economics shows that humans are predisposed to predictable biases that can lead to decision errors. Choice architecture utilizes some of these biases to direct individuals toward choices that are in their best interest by using "nudges". Nudges are parts of the choice architecture (e.g., words or visual stimuli) used to influence individual's choices, by structuring the choice assortment so that their cognitive biases are used to direct decision towards the desired outcome (Thaler & Sunstein, 2021).

Choice overload

Aligned with the common beliefs and neoclassical economic theory, research shows a positive relationship between a large array of choices and an increase in task performance, life satisfaction, intrinsic motivation, perceived control, personal autonomy, and well-being (Ryan & Deci, 2001). At the same time, aligned with the behavioral economics principles, studies conducted in marketing, public administration, political science, sociology, computer science, hospitality management, and medical science shows that when presented with a large variety of choices, people tend to experience a reduction in choice satisfaction and decision confidence, an increase in decision regret and switching likelihood, or even to completely defer the choice and postpone the decision (Chernev, et al., 2015). This puzzling effect was dubbed as "choice overload" (Iyengar & Lepper, 2000), "overchoice" (Gourville & Soman 2005), "too-much-choice effect" (Scheibehenne, et al., 2009), or "paradox of choice" (Schwartz, 2015).

Because of the counterintuitive nature of the findings showing that variety can be detrimental to choice with broad potential implications on various fields, choice overload attracted a significant amount of research interest. In an early study that helped popularize the choice overload concept (Iyengar & Lepper, 2000), researchers conducted an experiment offering varieties of jam in a tasting booth installed in a local grocery store. The products were offered in two separate sessions, with one presenting customers with twenty-four jam varieties and the other one with just six types of jam. Researchers found that 60% of store shoppers approached the jam tasting booth when presented with the extensive selection of twenty-four jams flavors, but only

3% of them ended up buying jam. On the other side, presenting shoppers with only six flavors of jam attracted only 40%, but resulted in 30% of them purchasing jam. Therefore, although the large variety of choices attracted people, they were more likely to make a purchasing decision when presented with a small selection of products. In the wake of Iyengar and Lepper (2000) findings, a multitude of similar studies were conducted within a variety of settings (e.g., marketing and sales, tourism, volunteering, investments, online dating, social welfare, healthcare). The results were inconsistent, with some studies supporting the choice overload hypothesis, but others rejecting it. Multiple recent meta-analytic reviews confirmed that the effect of the available number of options on choice overload is significant (Chernev et al., 2015; McShane, & Böckenholt, 2018; Zhang & Xu, 2019). The study conducted by Chernev and associates (2015) on 99 behavioral studies on choice overload proposed a conceptual model of the impact of available options on choice overload (Figure 1).

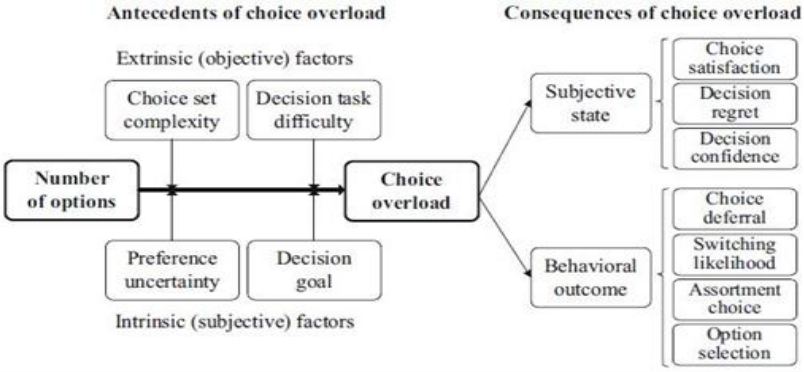

Figure 1. Conceptual Model of the Impact of Choice Assortment Size on Choice Overload. Source: Chernev et al. (2015)

Choice Overload and Decision Deferral in Cybersecurity

An extensive set of similar available choices leads to a higher incidence of decision paralysis and deferment probability (Redelmeier & Shafir, 1995). Choice overload can make individuals choose to postpone a decision and this can lead to not making a decision at all because people rarely revisit deferred decisions (Ariely & Wertenbroch, 2002). In organizational environments, decisions that are delaying compliance and security efforts are not delaying the risk. Decision deferral in the cybersecurity domain can lead to substantial negative consequences. For example, it is largely recognized that the key factor for the success of an attack employing SQL injection, drive-by-download, cross-site-scripting, buffer overflow, or social engineering are vulnerabilities created by postponing critical software updates (Rajivan, et al., 2020).

H1: In cybersecurity settings, individuals presented with a large assortment of choices are more likely to defer their decision than those that choose from a small assortment.

Despite concerns about the impact of time pressure influence on human behavior in cybersecurity settings, there is limited research in this area. Time constraints are included as a factor in the decision task difficulty moderator in the conceptual model of the impact of choice assortment size on choice overload presented in Figure 1 (Chernev et al., 2015). Counterintuitively, marketing research shows that time pressure can reduce the likelihood of decision deferment (Dhar & Nowlis, 1999). If similar findings are confirmed in cybersecurity, the implications are significant and would allow the implementation of methods to reduce decision deferral.

H2: In cybersecurity settings, decision deferral caused by choice overload is moderated by time constraints.

Based on the conceptual model of the impact of choice assortment size on choice overload presented in Figure 1 (Chernev et al., 2015), a simplified model was built to represent the relationship between the number of options, choice overload, and choice deferral, including time constraints as a moderator (Figure 2).

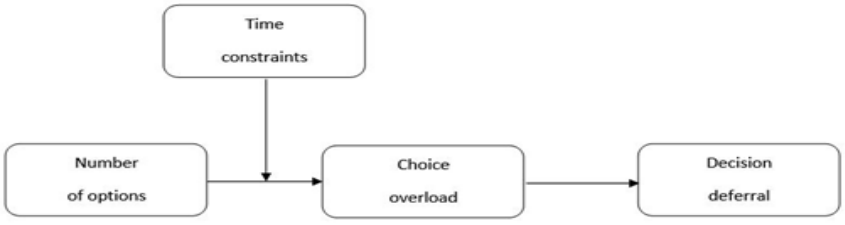

Figure 2. Conceptual Model of the Impact of Choice Assortment

METHODS

To assess the effects of the number of options and time constraints on decision deferral, we employed a 2 x 2 experimental design in which the number of options (small assortment of options versus large assortment of options) and the time constraints (limited decision time versus unlimited decision time) were manipulated between-participants. A total of 130 participants were recruited through Amazon Mechanical Turk (MTurk) and directed to complete the experimental tasks on Qualtrics in exchange for monetary compensation. Research generally finds that MTurk workers are demographically diverse and are a source of reliable data (Paolacci et al., 2010). G*Power 3.1.9.7 was used to determine the sample size for power (1-β err prob) = 0.80, effect size w = .25, α err prob = 0.05, df = 1. The resulting output parameters were: noncentrality parameter $\lambda = 7.875$, critical $\chi^2 = 3.8414588$, N = 126, actual power = 0.8013024.

A Qualtrics survey was set up to randomly assign an approximately equal number of participants to each of the four experimental conditions. Screening procedures were conducted to assure participants were at least 18 years of age and living in the United States. Multiple control measures were included in the experiment to ensure that the participants were fully understanding the requirements and, as an additional control measure for the quality of the participant pool, only MTurk workers with at least 500 completed HIT's and 95 percent approval rate were recruited for this study (Buhrmester et al., 2011). There were 298 attempts to complete this study: 130 usable responses, 154 incomplete surveys given that participants failed to pass the review questions, and 14 surveys with a duplicate MTurk ID. Of the participants, 52.30% were male, 46.90% female, and 0.80% non-binary. Participants' age: 23.17% were between 18 to 28 years old, 41.5% were between 29 and 38 years old, 18.46% were between 39 and 48 years old, 13.07% were between 49 and 58 years old, and 3.80% were between 59 to 69 years old. Participants' education: 16.04% were high school graduates, 13.85% had some college but no degree, 13.85% had an associate degree, 44.62% had a bachelor's degree, 9.24% had a master's degree, 0.80% had a professional degree, and 1.60% had doctoral degrees. Participants' employment: 49.25% were full-time employed, 17.70% were part-time employed, 23.85% were self-employed or business owners, 3.85% were full-time students, 3.85% were not employed but looking for work, and 1.59% were not employed and not looking for work.

The experiment required participants to choose a cybersecurity software suite, based on the available options. First, the participants were presented with a scenario placing them in the role of self-employed or small business owners who participated in a cybersecurity training offered by the U.S. Small Business Administration (SBA), a governmental organization dedicated to helping small business owners and entrepreneurs. The training presented them with information about cybersecurity risks and the potential negative effects on their business. At the end of the training, they were told that SBA offered all the participants, free of charge, a cybersecurity software suite license. Next, the participants were directed to an online page where the software suite options were presented and were announced that after they review the available cybersecurity software suite options, they can either let the SBA representative know the name of the cybersecurity software suite license they chose and claim their license immediately, or they can choose to get a certificate that allows them to make their choice at a later date and claim their software license during the next 30 days. The participants were randomly assigned to four conditions: 6 options, no time limit to decide; 6 options, 5 minutes to decide; 24 options, no time limit to decide, and 24 options, 5 minutes to decide. The number of options for the small and the large assortments were selected as identical with the levels used by Iyengar and Lepper (2000).

The collected data was coded as binary (6 choices/24 choices = 0/1; no time limit to decide/5 minutes to decide = 0/1; deferral/decision = 0/1). A Pearson's Chi-Square test was employed to evaluate the model using IBM© SPSS© Statistics Version 25. There was a statistically significant association between the number of options and whether a choice was made, or the decision was deferred ($\chi^2(1) = 15.111$, $p < .001$). Based on the odds ratio, the odds of deferring a decision on choosing a cybersecurity software suite were 4.33 times higher if people are presented with 24 options than if presented with 6 options. These findings confirm our hypothesis that individuals presented with a large assortment of choices are more likely to experience choice overload and consequently to defer their decision than individuals that choose from a small assortment.

In order to evaluate if decision deferral caused by choice overload is moderated by time constraints, we conducted a loglinear analysis that revealed a statistically significant 3-way interaction existed between the variables included in the model ($\chi^2(1) = 5.564$, $z = 2.290$, $p = .018$). The 2-way interaction between the number of options and whether a choice was made, or the decision was deferred was statistically significant ($\chi^2(1) = 16.597$, $z = 3.901$, $p < .001$). Also, the 2-way interaction between time constraints and whether a choice was made, or the decision was deferred is statistically significant ($\chi^2(1) = 4.973$, $z = 1.722$, $p = .026$). As expected, the 2-way interaction between time constraints and the number of options was not statistically significant ($\chi^2(1) = 1.120$, $z = .469$, $p = .483$). As Figure 3 shows, people were more inclined to make a choice (as opposed to defer the decision) if they were in a time-constrained situation than if no time constraint existed. The effect of the time constraints is especially visible in the case of individuals presented with a set of 24 options to choose from. These findings are supporting our second hypothesis, showing that decision deferral caused by choice overload is moderated by time constraints.

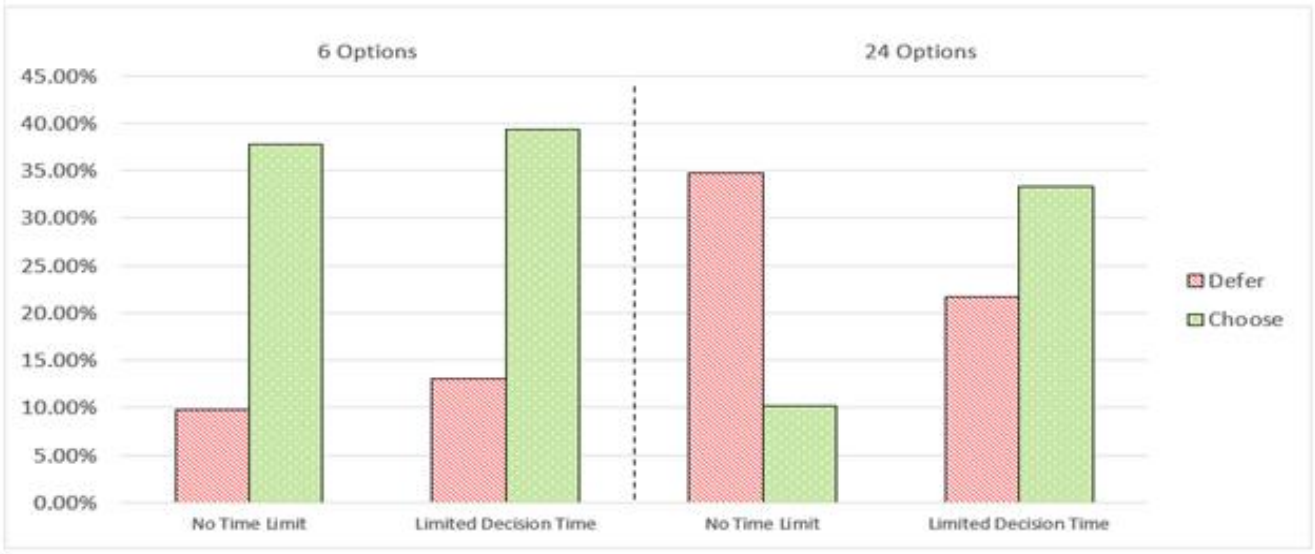

Figure 3. Visual interpretation of the loglinear model

DISCUSSION

The critical role of a human-centered approach is largely recognized in the cybersecurity research field, but we are still at an early stage of interdisciplinary research (Lahcen et. al, 2020). In order to accelerate the knowledge development in the behavioral cybersecurity area, we need to translate and adapt existent research from other scientific fields. This study examined the impact of choice overload bias on decision-making in cybersecurity settings and the influence of time constraints on this relation, based on a conceptual model of choice overload developed by Chernev and associates (2015) after reviewing 99 research papers from various fields (e.g., marketing, sales, tourism, volunteering, investments, online dating, social welfare, healthcare). In concordance with similar extant research grounded in behavioral economics conducted in other disciplines a statistically significant relationship between an extensive array of options and decision deferral caused by choice overload was found. Also, in line with our second hypothesis, we confirmed that time constraints moderate the relation between the number of choices and decision deferral.

The paper contributes to the behavioral cybersecurity research in several ways. Decision deferral as a result of the choice overload bias can have an important impact on cybersecurity. On one side, the delay in making a decision can lead to negative consequences. For example, postponing the decision to install software security updates can lead to security incidents. On the other side, choice overload bias can be used to increase cyber defense. For example, it can be employed as a potential cybersecurity attack deterrent with the attacker being affected by decision paralysis when presented with a large number of choices. In addition, our findings show that by utilizing a smaller array of options and introducing time constraints the adoption of cybersecurity software can be increased, with positive consequences for cybersecurity.

CONCLUSIONS

Building on behavioral economics principles this study extends research on choice overload to the cybersecurity area showing that when presented with a large assortment of choices individuals are more likely to defer their decision than when presented with a small assortment of choices. In addition, we demonstrate that time constraints are acting as a moderator in the relationship between the number of choices and decision deferral caused by choice overload, with the odds of decision deferral decreasing when a limited decision time is introduced.

Future research in this area might consider examining the potential negative influence of time constraints on the decision quality. Additionally, an exploration of the moderation effects using a continuous time constraints variable can further help expand the understanding and applications of these findings in cybersecurity.

REFERENCES

1. Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information & Computer Security*, *24*(2), 205–227.
2. Ariely, D. (2009). The end of rational economics. *Harvard business review*, *87*(7-8), 78-84.

3. Ariely, D., & Wertenbroch, K. (2002). Procrastination, Deadlines, and Performance: Self-Control by Precommitment. *Psychological Science*, *13*(3), 219–224.
4. Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk. *Perspectives on Psychological Science*, *6*(1), 3–5.
5. Cano, J. J (2019). The Human Factor in Information Security. *ISACA Journal*, (Vol.5).
6. Chernev, A., Böckenholt, U., & Goodman, J. (2015). Choice overload: A conceptual review and meta-analysis. *Journal of Consumer Psychology*, *25*(2), 333–358.
7. Dhar, R., & Nowlis, S. (1999). The Effect of Time Pressure on Consumer Choice Deferral. *Journal of Consumer Research*, *25*(4), 369–384.
8. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, *30*(1), 28–38.
9. Gigerenzer, G., & Selten, R. (2002). *Bounded rationality: The adaptive toolbox*. MIT press.
10. Iyengar, S. S., & Lepper, M. R. (2000). When choice is demotivating: Can one desire too much of a good thing? *Journal of Personality and Social Psychology*, *79*(6), 995–1006.
11. Kahneman, D. (2011). *Thinking, Fast and Slow*. New York: Macmillan.
12. Klaes, M., & Sent, E. M. (2005). A Conceptual History of the Emergence of Bounded Rationality. *History of Political Economy*, *37*(1), 27–59.
13. Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1).
14. Lyons, A., & Kass-Hanna, J. (2021). Behavioral Economics and Financial Decision Making. *SSRN Electronic Journal*. Published.
15. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, *147*, 424–428.
16. McShane, B. B., & Böckenholt, U. (2017). Multilevel Multivariate Meta-analysis with Application to Choice Overload. *Psychometrika*, *83*(1), 255–271.
17. Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88.
18. Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on Amazon Mechanical Turk. *Judgment and Decision making*, *5*(5), 411-419.
19. Rajivan, P., Aharonov-Majar, E., & Gonzalez, C. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. *Journal of Cybersecurity*, *6*(1).
20. Redelmeier, D. A. & Shafir, E. (1995). Medical decision making in situations that offer multiple alternatives. *JAMA: The Journal of the American Medical Association*, *273*(4), 302–305.
21. Ryan, R. M., & Deci, E. L. (2001). On happiness and human potentials: A review of research on hedonic and eudaimonic well-being. *Annual review of psychology*, *52*(1), 141-166.
22. Scheibehenne, B., Greifeneder, R., & Todd, P. M. (2009). What moderates the too-much-choice effect? *Psychology and Marketing*, *26*(3), 229–253.
23. Schultz, E. (2005). The human factor in security. *Computers & Security*, *24*(6), 425–426.
24. Schwartz, B. (2015). The paradox of choice. Positive Psychology in Practice: Promoting Human Flourishing in Work, Health, Education, and Everyday Life, Second Edition, 121-138.
25. Thaler, R. H., & Sunstein, C. R. (2021). *Nudge: The final edition*. Penguin.
26. Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124–1131.
27. Wiederhold, B. K. (2014). The Role of Psychology in Enhancing Cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, *17*(3), 131–132.
28. Zhang, N., & Xu, H. (2019). Reconciling the Paradoxical Findings of Choice Overload Through an Analytical Lens. *MIS Quarterly (Forthcoming)*.