The Journal of the Southern Association for Information Systems

Volume 10 | Issue 2 Article 1

11-2-2023

The Impact of Choice Overload on Decision Deferral in Cybersecurity

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

Recommended Citation

Alecse, C. (2023). The Impact of Choice Overload on Decision Deferral in Cybersecurity. The Journal of the Southern Association for Information Systems, 10, 1-11. https://doi.org/doi:10.17705/3JSIS.00032

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 (Dhar, 1997; Shafir, Simonson and Tversky, 1993). Choice overload bias, also known as over-choice, choice paralysis, or the paradox of choice, describes how individuals get overwhelmed when presented with a large number of options to choose from. While we tend to assume that more choice is a good thing (Ryan and Deci, 2001), behavioral economics related research has shown that people have a harder time choosing from a larger array of options (Chernev, Böckenholt and Goodman, 2015). 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, Islam and Mouratidis, 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 (Morgan, 2016) are largely disproportionate compared with the relatively small amounts allocated to mitigate human-related security issues (Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas and Giannakopoulos, 2014). This approach is generally aligned with the neoclassical (standard) economics model of 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). Therefore, the information security frameworks adopted by organizations largely include 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 a 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 often deviate from the rational-choice model (Thaler and Sunstein, 2021). Accepting humans as bounded-rationality agents allows us to probe why people are not always making “rational” or “optimal” decisions, even in the conditions when they have a direct benefit to do it (Klaes and 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, Caulkins, Mohapatra and Kumar, 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, Sharma, Mahoney, Sousan, Zhu and Laplante, 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 (Lahcen, et. al, 2020; Nobles, 2018) confirm that we are still in the incipient stage of 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

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 and 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, employs 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 and Kahneman, 1974). This can result in irrational behavior and erroneous choices (Gigerenzer and 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.

DOI: doi:10.17705/3JSIS.00032

Choice architecture

Choice architecture describes how different presentations of choices can influence individuals' decision-making (Thaler and Sunstein, 2021) 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 choice structuring, creating incentives for taking decisions, or limiting the number of choices presented for decision (Thaler, Sunstein, and Balz, 2013).

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 and Sunstein, 2021).

Exploiting human biases by using nudges in decision-making can create questions about the ethics of limiting an individual's autonomy and freedom of choice and introduce the danger that if used in a devious manner it can lead people to decisions that are not in their best interest (Smith, Goldstein and Johnson, 2013). This can be avoided by using nudging in a transparent, non-misleading way, by giving the possibility to opt-out of a nudge, and by making sure nudges are only used to direct decisions in the benefit of the individual (Thaler and 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 and 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 and Lepper, 2000), "overchoice" (Gourville and Soman 2005), "too-much-choice effect" (Scheibehenne, Greifeneder and Todd, 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 in various fields, choice overload attracted a significant amount of research interest. In an early study that helped popularize the choice overload concept (Iyengar and Lepper, 2000), researchers conducted an experiment offering varieties of jams 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 jam 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's (2000) findings, a multitude of similar studies were conducted within a variety of settings: marketing and sales (e.g., Chernev 2003; Fasolo, Carmeci and Misuraca, 2009; Schwartz, 2016; Sela, Berger and Liu, 2009), tourism (e.g., Chernev, 2006; Goodman and Malkoc, 2012; McCabe, Li and Chen, 2016; Park and Jang, 2013), volunteering (e.g., Carroll, White and Pahl, 2011), investments (e.g., Iyengar and Kamenica, 2010; Morrin et al., 2012; Scheibehenne et al., 2009), online dating (e.g., Pronk and Denissen, 2020), social welfare (e.g., Botti and Iyengar, 2006), and healthcare (e.g., Patrick et al., 2019). The results were inconsistent, with some studies supporting the choice overload hypothesis, but others rejecting it. An early meta-analytic review of the choice overload research "found a mean effect size of virtually zero" (Scheibehenne, Greifeneder and Todd, 2010), but the conclusions were contested (Chernev, Böckenholt, and Goodman, 2010). 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 and Böckenholt, 2018; Zhang and 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).

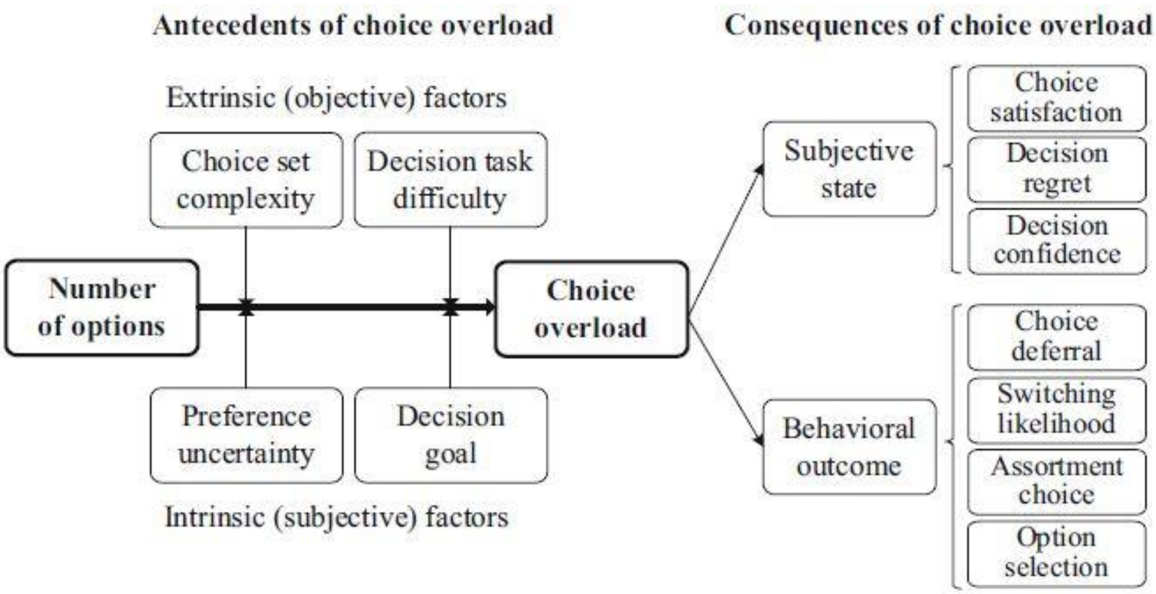

Figure 1. Conceptual Model of the Impact of Choice Assortment Size on Choice Overload (Chernev et al., 2015)

Note. The four antecedents of choice overload are operationalized as follows: (i) The complexity of the choice set describes the aspects of the decision set associated with the particular values of the choice options: the presence of a dominant option in the choice set, the overall attractiveness of the options in the choice set, and the relationship between individual options in the decision set (alignability and complementarity); (ii) the difficulty of the decision task refers to the general structural characteristics of the decision problem: time constraints, decision accountability, and number of attributes describing each option; (iii) preference uncertainty refers to the degree to which individuals have articulated preferences with respect to the decision at hand and has been operationalized by two factors: the level of product-specific expertise and the availability of an articulated ideal point; and (iv) the decision goal reflects the degree to which individuals aim to minimize the cognitive effort involved in making a choice among the options contained in the available choice sets and is operationalized by two measures: decision intent (buying vs. browsing) and decision focus (choosing a choice set vs. choosing a particular option). In this context, we expect higher levels of decision task difficulty, greater choice set complexity, higher preference uncertainty, and a more prominent, effort-minimizing goal to produce greater choice overload. Source: Chernev et al. (2015), Figure 1.

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 and Shafir, 1995). Choice overload can make individuals choose to postpone a decision, leading to not making a decision at all because people rarely revisit deferred decisions (Ariely and Wertenbroch, 2002). In organizational environments, decisions that are delaying compliance and security efforts are not delaying the risk (Posey and Canham, 2018). Decision deferral in the cybersecurity domain can lead to substantial negative consequences (Blau, 2017). For example, it is largely recognized that the key factor for the success of several cyberattack methods (e.g., SQL injection, drive-by-download, cross-site-scripting, buffer overflow, or social engineering) are vulnerabilities created by postponing critical software updates (Rajivan, Aharonov-Majar and Gonzalez., 2020).

Hypothesis 1: 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 (Chowdhury, Adam and Skinner, 2019). 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 and Nowlis, 1999). If similar findings are confirmed in cybersecurity, the implications are significant and would allow the implementation of methods to reduce decision deferral.

Hypothesis 2: 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 moderator (Figure 2).

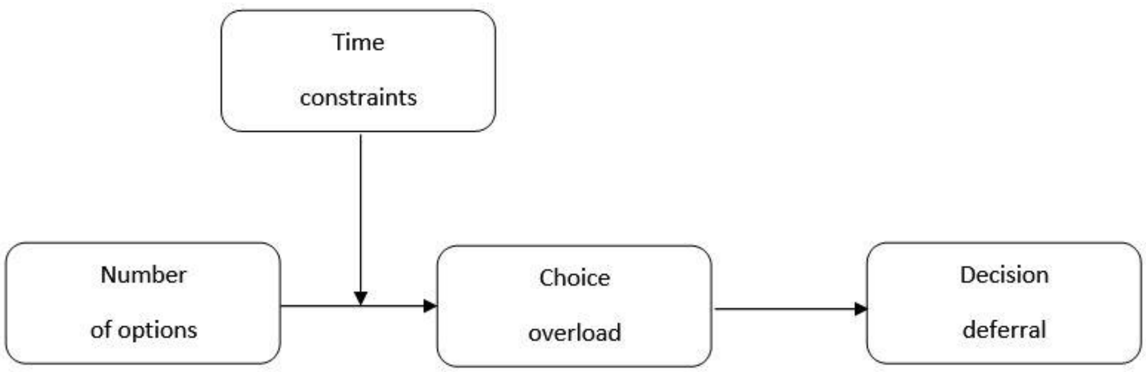

Figure 2. Model of Choice Deferral as Result of Choice Overload in Cybersecurity

METHODS

To assess the effects of the number of options and time constraints on decision deferral, we employed a 2 x 2 between-subjects 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.

The 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 (Buhrmester, Kwang and Gosling, 2011; Paolacci, Chandler and Ipeirotis, 2010). G*Power 3.1.9.7 software application was used to determine the sample size for power ($1-\beta$ 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 = 130, 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. Attention checks were placed 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 HITs and a 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 session 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 several software suite options were presented and it was 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 was selected as identical to 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 ($\chi2(1) = 15.111$, $p < .001$). 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 the Hypothesis 1 that individuals presented with a large assortment of choices are more likely to experience choice overload and consequently 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 (Hypothesis 2), we conducted a loglinear analysis that revealed a statistically significant 3-way interaction existed between the variables included in the model ($\chi2(1) = 5.564$, $z = 2.290$, $p = .018$). The 2-way interaction between the number of options and whether a choice was made, or the decision was deferred was statistically significant ($\chi2(1) = 16.597$, $z = 3.901$, $p < .001$). Also, the 2-way interaction between time constraints and whether a choice was made, or the decision was deferred is statistically significant ($\chi2(1) = 4.973$, $z = 1.722$, $p = .026$). As expected, the 2-way interaction between time constraints and the number of options was not statistically significant ($\chi2(1) = 1.120$, $z = .469$, $p = .483$).

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 support the second hypothesis, showing that decision deferral caused by choice overload is moderated by time constraints.

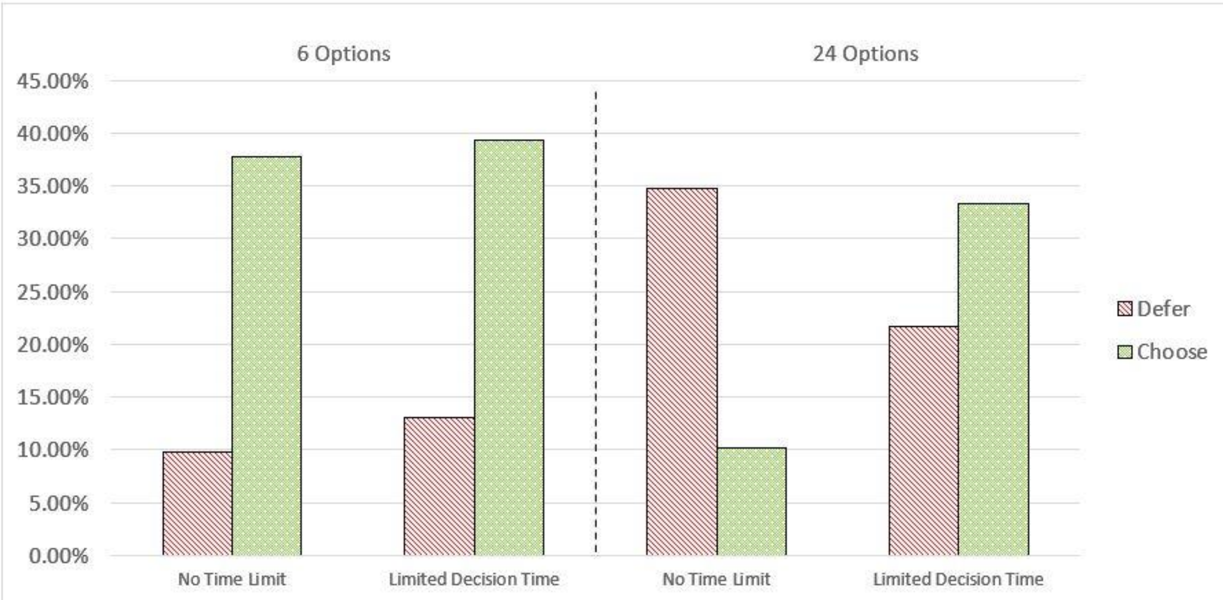

Figure 3. Visual interpretation of the loglinear model

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 existing 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).

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 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., and Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. Information and Computer Security, 24(2), 205–227. https://doi.org/10.1108/ics-01-2016-0006
2. Ariely, D. (2009). The end of rational economics. Harvard business review, 87(7-8), 78-84.
3. Ariely, D., and Wertenbroch, K. (2002). Procrastination, Deadlines, and Performance: Self-Control by Precommitment. Psychological Science, 13(3), 219–224. https://doi.org/10.1111/1467-9280.00441
4. Blau, A. (2017). Better cybersecurity starts with fixing your employees' bad habits. Harvard Business Review. Retrieved October 10, 2021, from https://hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits
5. Botti, S., and Iyengar, S. S. (2006). The Dark Side of Choice: When Choice Impairs Social Welfare. Journal of Public Policy and Marketing, 25(1), 24–38. https://doi.org/10.1509/jppm.25.1.24
6. Buhrmester, M., Kwang, T., and Gosling, S. D. (2011). Amazon's Mechanical Turk. Perspectives on Psychological Science, 6(1), 3–5. https://doi.org/10.1177/1745691610393980
7. Cano, J. J (2019). The Human Factor in Information Security. ISACA Journal, (Vol.5).
8. Carroll, L. S., White, M. P., and Pahl, S. (2011). The impact of excess choice on deferment of decisions to volunteer. Judgment and Decision Making, 6(7), 629. Retrieved October 10, 2021, from http://journal.sjdm.org/11/11418/jdm11418.pdf
9. Chernev, A. (2003). When More Is Less and Less Is More: The Role of Ideal Point Availability and Assortment in Consumer Choice. Journal of Consumer Research, 30(2), 170–183. https://doi.org/10.1086/376808
10. Chernev, A., Böckenholt, U., and Goodman, J. (2010). Commentary on Scheibehenne, Greifeneder, and Todd Choice Overload: Is There Anything to It? Journal of Consumer Research, 37(3), 426–428. https://doi.org/10.1086/655200
11. Chernev, A., Böckenholt, U., and Goodman, J. (2015). Choice overload: A conceptual review and meta-analysis. Journal of Consumer Psychology, 25(2), 333–358. https://doi.org/10.1016/j.jcps.2014.08.002
12. Chowdhury, N. H., Adam, M. T. P., and Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: a systematic literature review. Behaviour and Information Technology, 38(12), 1290–1308. https://doi.org/10.1080/0144929x.2019.1583769
13. Dhar, R. (1997). Consumer Preference for a No-Choice Option. Journal of Consumer Research, 24(2), 215–231. https://doi.org/10.1086/209506
14. Dhar, R., and Nowlis, S. (1999). The Effect of Time Pressure on Consumer Choice Deferral. Journal of Consumer Research, 25(4), 369–384. https://doi.org/10.1086/209545
15. Fasolo, B., Carmeci, F. A., and Misuraca, R. (2009). The effect of choice complexity on perception of time spent choosing: When choice takes longer but feels shorter. Psychology and Marketing, 26(3), 213–228. https://doi.org/10.1002/mar.20270
16. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. IEEE Technology and Society Magazine, 30(1), 28–38. https://doi.org/10.1109/mts.2011.940293
17. Gigerenzer, G., and Selten, R. (2002). Bounded rationality: The adaptive toolbox. MIT press.

18. Goodman, J. K., and Malkoc, S. A. (2012). Choosing Here and Now versus There and Later: The Moderating Role of Psychological Distance on Assortment Size Preferences. Journal of Consumer Research, 39(4), 751–768. https://doi.org/10.1086/665047
19. Gourville, J. T., and Soman, D. (2005). Overchoice and Assortment Type: When and Why Variety Backfires. Marketing Science, 24(3), 382–395. https://doi.org/10.1287/mksc.1040.0109
20. Kahneman, D. (2011). Thinking, Fast and Slow. New York: Macmillan.
21. Klaes, M., and Sent, E. M. (2005). A Conceptual History of the Emergence of Bounded Rationality. History of Political Economy, 37(1), 27–59. https://doi.org/10.1215/00182702-37-1-27
22. Iyengar, S. S., and 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. https://doi.org/10.1037/0022-3514.79.6.995
23. Iyengar, S. S., and Kamenica, E. (2010). Choice proliferation, simplicity seeking, and asset allocation. Journal of Public Economics, 94(7–8), 530–539. https://doi.org/10.1016/j.jpubeco.2010.03.006
24. Lahcen, R. A., Caulkins, B., Mohapatra, R., and Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(1). https://doi.org/10.1186/s42400-020-00050-w
25. Lyons, A., and Kass-Hanna, J. (2021). Behavioral Economics and Financial Decision Making. SSRN Electronic Journal. Published. https://doi.org/10.2139/ssrn.3887605
26. McCabe, S., Li, C. S., and Chen, Z. (2015). Time for a Radical Reappraisal of Tourist Decision Making? Toward a New Conceptual Model. Journal of Travel Research, 55(1), 3–15. https://doi.org/10.1177/0047287515592973
27. McShane, B. B., and Böckenholt, U. (2017). Multilevel Multivariate Meta-analysis with Application to Choice Overload. Psychometrika, 83(1), 255–271. https://doi.org/10.1007/s11336-017-9571-z
28. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, 147, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133
29. Morgan, S. (2016). Top 5 industries at risk of cyberattacks. Forbes.com. Retrieved on October 17, 2021, from https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/?sh=9300c0f715e9
30. Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. HOLISTICA – Journal of Business and Public Administration, 9(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024
31. Paolacci, G., Chandler, J., and Ipeirotis, P. G. (2010). Running experiments on Amazon Mechanical Turk. Judgment and Decision making, 5(5), 411-419. http://journal.sjdm.org/10/10630a/jdm10630a.pdf
32. Park, J. Y., and Jang, S. S. (2013). Confused by too many choices? Choice overload in tourism. Tourism Management, 35, 1–12. https://doi.org/10.1016/j.tourman.2012.05.004
33. Posey, C., and Canham, M. (2018). A computational social science approach to examine the duality between productivity and cybersecurity policy compliance within organizations. In International Conference on Social Computing, Behavioralcultural Modeling and Prediction and Behavior Representation in Modeling and Simulation (SBP-BRiMS). Retrieved on October 17, 2021 from http://sbp-brims.org/2018/proceedings/papers/latebreaking_papers/LB_1.pdf
34. Pronk, T. M., and Denissen, J. J. A. (2019). A Rejection Mind-Set: Choice Overload in Online Dating. Social Psychological and Personality Science, 11(3), 388–396. https://doi.org/10.1177/1948550619866189
35. Rajivan, P., Aharonov-Majar, E., and Gonzalez, C. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. Journal of Cybersecurity, 6(1). https://doi.org/10.1093/cybsec/tyaa002

36. Redelmeier, D. A. and Shafir, E. (1995). Medical decision making in situations that offer multiple alternatives. JAMA: The Journal of the American Medical Association, 273(4), 302–305. https://doi.org/10.1001/jama.273.4.302
37. Ryan, R. M., and 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.
38. Sela, A., Berger, J., and Liu, W. (2009). Variety, Vice, and Virtue: How Assortment Size Influences Option Choice. Journal of Consumer Research, 35(6), 941–951. https://doi.org/10.1086/593692
39. Scheibehenne, B., Greifeneder, R., and Todd, P. M. (2009). What moderates the too-much-choice effect? Psychology and Marketing, 26(3), 229–253. https://doi.org/10.1002/mar.20271
40. Scheibehenne, B., Greifeneder, R., and Todd, P. M. (2010). Can There Ever Be Too Many Options? A Meta-Analytic Review of Choice Overload. Journal of Consumer Research, 37(3), 409–425. https://doi.org/10.1086/651235
41. Schultz, E. (2005). The human factor in security. Computers and Security, 24(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002
42. 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.
43. Shafir, E., Simonson, I., and Tversky, A. (1993). Reason-based choice. Cognition, 49(1-2), 11-36.
44. Smith, N. C., Goldstein, D. G., and Johnson, E. J. (2013). Choice without Awareness: Ethical and Policy Implications of Defaults. Journal of Public Policy and Marketing, 32(2), 159–172. https://doi.org/10.1509/jppm.10.114
45. Thaler, R. H., and Sunstein, C. R. (2021). Nudge: The final edition. Penguin.
46. Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2013). Choice architecture. The behavioral foundations of public policy, 25, 428-439.
47. Tversky, A., and Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. Science, 185(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124
48. Wiederhold, B. K. (2014). The Role of Psychology in Enhancing Cybersecurity. Cyberpsychology, Behavior, and Social Networking, 17(3), 131–132. https://doi.org/10.1089/cyber.2014.1502
49. Zhang, N., and Xu, H. (2019). Reconciling the Paradoxical Findings of Choice Overload Through an Analytical Lens. MIS Quarterly (Forthcoming). Retrieved October 10, 2021, from https://misq.org/reconciling-the-paradoxical-findings-of-choice-overload-through-an-analytical-lens.html

ABOUT THE AUTHOR

Cristian Alecse, Ph.D. is a faculty in the College of Business, at the University of Central Florida. His research interest is in the information systems area, particularly in behavioral cybersecurity and human behavior influence on artificial intelligence.