Deciding to Fail: Three Essays about Self-Interest in Systems

DECIDING TO FAIL: THREE ESSAYS ABOUT SELF-INTEREST IN SYSTEMS

BY

PENGCHENG WANG

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree

Of

Doctor of Philosophy

In the Robinson College of Business

Of

Georgia State University

GEORGIA STATE UNIVERSITY

ROBINSON COLLEGE OF BUSINESS

2022

ACCEPTANCE

This dissertation was prepared under the direction of the PENGCHENG WANG's Dissertation Committee. It has been approved and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business Administration in the J. Mack Robinson College of Business of Georgia State University.

Richard Phillips, Dean

DISSERTATION COMMITTEE

Dr. Richard Baskerville (Chair)

Dr. Likoebe Maruping (Member)

Dr. Dmitry Zhdanov (Member)

Dr. Youngjin Yoo (External Member)

ABSTRACT

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree

By

Pengcheng Wang

August 12, 2022

Committee Co-Chairs: Dr. Richard Baskerville
Major Academic Unit: Computer Information Systems

Information technologies (ITs) are designed with intended functions to support human and organizational purposes. Human agents may interpret and use the technologies in ways beyond their original intent, which may cause unanticipated consequences that diminish IT's holistic value, causing the information systems to become less sustainable. The information systems field mainly focuses on analyzing how IT is developed, applied to, and shaped in social situations. While many studies examine how individuals and organizations value the flexibility provided by IT in complex business and social environments and what are the actual effects of IT uses, less attention has been paid to how IT's flexibility and individuals' autonomy could potentially generate information systems failure points. This thesis examines the system failure point caused by the tension between individual self-interest decisions and retaining information system sustainability during the IT design, development, and implementation. The overarching theme in this dissertation is, can we explain how individual actions, resulting from individual rational decisions respect, or fail to respect, the principle of rational decisions at the system (or collective) level? In other words, what are the negative impacts of individual rational decisions on information system sustainability? This thesis encompasses three independent research papers reflecting my diverse approach to this research theme. Indeed, the theme emerged from the work conducted in these three studies rather than the other way round. This thesis aims to advance the information systems literature and digitalization by providing fresh views on how individual decisions in the different contexts of IT design, development, and implementation may introduce system weakness and failure points.

ACKNOWLEDGEMENT

First and foremost, I would like to thank my committee chair, lifetime mentor, friend, and role model, Dr. Richard Baskerville, for his excellent guidance and support throughout my Ph.D. program. I am lucky to have Richard as my supervisor, and I enjoy every single second I spend with Richard. I still remember the first time I met with Richard, and he was patiently listening to my unmatured research ideas. He teaches me how to challenge the obvious, propose interesting research questions, and guide me through every research project I would like to explore. I sincerely appreciate Richard has faith in me and has encouraged me during my Ph.D. journey. Without Richard, I could not make this dissertation possible. He will always be my role model and inspire me to be a great scholar. Thank you, Richard, for everything!

I want to thank my committee members, Dr. Likoebe Maruping, Dr. Dmitry Zhdanov, and Dr. Youngjin Yoo. Thank you all so much for helping me make this dissertation and my defense possible. I first met Dr. Maruping during my Ph.D. application process, and his smiles and wisdom gave me the confidence that I am going to get the best possible research training I could imagine at Georgia State University. I want to thank Dr. Zhadnove for sharing his cybersecurity course teaching materials and for his guidance during my dissertation process. I want to thank Dr. Yoo for his great help in inspiring my ethnographic study. Without his wisdom on service-dominant logic, I could not make the last chapter possible.

I want to thank all faculty members of the Computer Information Systems department. Thank you all for making our department such an enjoyable place to work. I especially want to thank Dr. Mark Keil, who admitted me into the Ph.D. Program. Dr. Keil is always my role model, and I hope one day I can become a great scholar like Dr. Keil. I also want to thank our department Chair, Dr. Balasubramaniam Ramesh. Thank you, Dr. Ramesh, offered unconditional support

during the most difficult time in my last year. My special thanks go to my fellow doctoral students at the Computer Information System department. It was my great honor to work with you guys.

Last but not least, I want to thank my family, especially my wife, Lan Xia. Without her love, inspiration, encouragement, and unconditional support, I would not have been at this stage of my career. Thank you, Lan, for taking over my family responsibilities so that I can pursue my Ph.D. dream. Thank you all that I forgot to mention.

DECIDING TO FAIL: THREE ESSAYS ABOUT SELF-INTEREST IN SYSTEMS

Table of Contents

Chapter 1. Thesis Introduction

1.1 Motivation and Objective of Dissertation

Digitalization is a socio-technical process of applying information technologies (IT) to facilitate social and institutional processes (Tilson et al., 2010). The inherent flexibility and scalability of IT make it possible to foster digitalization growth to an extraordinary scale and scope. As a result, information technology has permeated practically every facet of human activity (Baskerville et al., 2020; Recker et al., 2021; Yoo, 2010). Indeed, the creation of IT is no longer limited to the purpose of simply reflecting reality; rather, it progressively modifies, mediates, and even generates reality. (Baskerville et al., 2020; Recker et al., 2021).

There is no doubt that digitalization benefits us in many ways. While enjoying the benefits of digitalization, we are continually confronted with an increasing number of unanticipated consequences, such as the rapid spread of fake news (Vosoughi et al., 2018), polarization (Shore et al., 2018), and IT addition (Turel et al., 2011). Those examples of unanticipated consequences show how IT deployment and appropriation are contingent on the social and economic context that is independent of its design purposes. These contingencies may thwart the success of IT implementation (DeLone & McLean, 1992, 2003) and diminish IT's holistic value (Klein & Hirschheim, 1985).

The information systems field focuses on analyzing how IT is developed, applied to, and shaped in social situations (Grover & Lyytinen, 2015). While many studies examine how individuals and organizations value the flexibility provided by IT in complex business and social environments and what are the actual effects of IT uses (see Burton-Jones et al. (2017) for IT use summary), less attention has been paid to how the IT's flexibility and individuals' autonomy could potentially generate information *systems failure points*. Indeed, IT can be created in a way that contains the

seeds of its own destruction, preventing essential social activities that hold organizational elements together (Baskerville & Land, 2004). Baskerville and Land (2004) posit that IT can be self-destructive in two ways: inwardly destructive or outwardly destructive. The inwardly destructive IT can destroy the information systems internally into isolated parts by degrading the information system performance or causing system failure. In comparison, outwardly destructive IT can destroy the organizational context of the information systems by breaking down organizational structure that forces the organizational components apart. This dissertation focuses on the inwardly destructive IT that downgrading the performance of the information system through creating the system failure points.

In this study, drawing the literature on information system reliability (Butler & Gray, 2006; Zahedi, 1987), I define the ***system failure point*** as the introduced information systems points of vulnerability caused by individual users' self-interest decisions that make it less likely that the system will achieve its goals in a given period of time and under a given set of conditions. An information system is not just the IT artifacts but also the hardware, infrastructure, application systems, human agents, and many other elements that collectively operate to produce effects (Davis, 2000). Thus, drawing the social-technical view, I no longer view the information technology and system users as isolated entities but view the information system as a social-technical system that is made of two jointly independent but correlative interacting systems, which are social and technical systems (Bostrom & Heinen, 1977a, 1977b). Under this view, the performance of the information system is the result of joint interactions between and within system users and technology artifacts (Baird & Maruping, 2021). Therefore, to understand the system failure points, we cannot not only examine IT alone because there are always social-system

elements and IT elements to be considered in the information system design, development, and implementation (Davis et al., 1992).

In theoretical debates on IS operations, design, and management, the paradox of depending on complex systems with unreliable components to provide dependable results is seldom addressed. IS research tends to assume a best-case scenario regarding the dependability of information systems, concentrating on approaches for obtaining dependable performance via the construction of technically reliable information systems from organized combinations of components.

This dissertation examines the system failure point caused by the tension between individual self-interest decisions and retaining information system sustainability during the information system design (Chapter 3), development (Chapter 4), and implementation (Chapter 2). According to the Cambridge Dictionary, sustainability in its broadest sense refers to "*the quality of being able to continue over time*." Thus, ***the sustainability of IT*** can be best defined as IT's ability to be able to continue being used over a period of time. Different users will interpret a certain IT differently (Orlikowski, 1992), so their use of the IT will reflect and develop diverse interests. Thus, IT will inevitably meet with unanticipated conditions and, through use, will generate unanticipated consequences, introducing aggerated vulnerabilities (see Mindel et al. (2018) as an example) that endanger IT's long-term sustainability.

Should we curtail individual freedom on IT use? The modern economic founding father Adam Smith, in his seminal book, An Inquiry Into the Nature and Causes of the Wealth of Nations (Smith, 1786), uses a metaphor, the invisible hand, to describe how people act and make rational decisions in their self-interest can lead to the greater social and public welfare. Following Adam Smith's logic, he would suggest that IT users are the best judge of their own advantage and needs, so it would be the society's best interest for the individual to pursue the use of IT without intervention

or hindrance. It is worth noting that self-interest decisions do not equal selfish decisions. In Adam Smith's early book, The Theory of Moral Sentiments (Smith, 1761), he points out that people want to be respected by themselves and by others. He thinks that this respect comes from people acting honestly, fairly, and caring toward others in their community. So, individual behaviors will be self-regulated by *moral sentiments*, which is the universal desire for self-respect and the respect of others. However, individual self-interest and rational decision-making may not always lead to desirable collective outcomes. For instance, in the Ultimatum Game (Güth et al., 1982), the responder and proposer are in a take-it-or-leave-it bargaining environment. The proposer has money to split with his responder, and the responder considers the money division suggestion and acts accordingly. If the division is accepted, each earns the amount suggested. If denied, both parties get nothing. Güth et al. (1982) find that the responder would rather walk away with nothing than be treated in a way they perceive as unfair, even though accepting whatever suggested money division is always a better collection outcome.

Translating those findings from economic literature into an information systems context, we cannot simply give individuals the freedom to decide how IT is used without considering its embedded system context. IT's inherent flexibility allows it to satisfy individual users' heterogeneous needs but can also cause it to lose its connection with its users. This limits users' freedom to decide without being controlled by or influencing other systems parts (Baird & Maruping, 2021). In other words, individuals' rational decisions in their own self-interests cannot always lead to a greater systemwide outcome. Such decisions may introduce the system's weakness and failure points that diminish its long-term sustainability. Indeed, the existing information system literature indicates that the implementation of IT can cause IT users to be trapped in the *Prisoner's Dilemma* (Dewan et al., 2000). For instance, Dewan et al. (2000) find

that adopting advanced manufacturing IT and Internet technologies can improve sellers' flexibility in manufacturing customized products, allowing them to charge a high premium from the consumer, increasing the sellers' profits. However, the benefits of IT afforded customization on consumer's products will soon disappear when more competitors adopt customization, trapping all the manufacturers in the same market segment into a prisoner's dilemma because all rational manufacturers must adopt or keep offering the product customization in order to retain their competitive advantages. Consequently, the profits are lower when the manufacturers offer product customization than when they do not.

The overarching theme in this research is, *can we explain how individual actions, resulting from individual rational decisions, respect, or fail to respect, the principle of rational decisions at the system (or collective) level?* In other words, w*hat are the negative impacts of individual rational decisions on information system sustainability?*

The structure of this thesis

This thesis encompasses three quite independent research papers that reflect my diverse approach to this research theme. Indeed, the theme emerged from the work conducted in these three projects rather than the other way round. For each paper (chapters 2-4), I provide a chapter preface and a chapter postscript that explains how the research framing and results address the overarching theme embodied by this thesis.

I should acknowledge that I do not intend to find a universal solution to fit all information sustainability issues but rather examine how individual decisions in IT use contexts may introduce system weakness and failure points. Indeed, Orlikowski (1992) suggests that IT may be modified over the course of its existence, and an analytical distinction needs to be drawn between users'

actions and decisions that influence IT. This analytical distinction is useful when attempting to comprehend IT as something that is constantly being socially and physically constructed. Therefore, this dissertation consists of three subsequent research questions to guide my three individual essays in various information system contexts. Specifically, those three questions are:

1. *How could system users' rational security decisions endanger the reliability of information security systems?*
2. *How could researchers' rational decision on designing a new two-factor authentication artifact introduce more or less embedded risks?*
3. *How could IT afford flexibility on digital resources provision and appropriation to create the emergence of free-riding?*

1.2 Overview of Three Essays

Chapter 2 is a quantitative research study examining the negative consequences of the adoption of information security technology by presenting the paradoxical relationship between information security technologies and actual system security risks. In this study, I theorize that information security technologies' protection benefits could be simultaneously diminished by system user risk-taking decisions when adopting new information security technologies into organizations. Drawing insights from the Carver and Scheier (1982) theory of self-regulation, I theorize the system user's security behavior as a part of self-regulated systems and that user security behavior influences and is being influenced by their surrounding security environment. I find that the individual's perception of the system security environment, and their corresponding security behavior, condition the effects of information security technologies through two divergent paths: expected utility of a security action decision and expected utility of an insecurity action decision. In this study, I conclude, through an experimental study, that although information security

technology makes the system's security environment safer, the system user's risk-taking behavior can negatively compensate for the system's security environment change, canceling out protection benefits of the security technologies and reducing information security system's reliability.

Table 1-1. Outline of Research Essays

Essay Title	Context	Theoretical Background	Methodology
Chapter 2 When security technologies backfire: the behavioral tradeoff between information system functionality and information system security	Information Security	Self-regulation Theory and Expected Utility Theory	Experiments
Chapter 3 The case for two-factor authentication- Evidence from a literature review	Security Technology	Two-Factor Authentication	Literature review
Chapter 4 When digital equality creates inequality: making open digital resource systems sustainable	Online Communities	Commons Resource Management and Service-Dominant Logic	Ethnography

Chapter 3 is a literature review and serves as a supplement to chapter 2. In this study, I zoom into cybersecurity literature to see how cybersecurity scholars see the effectiveness of two-factor authentication technology in reducing cybersecurity risks. Specifically, I investigate what is currently known about the benefits and limitations of two-factor authentication and how additional authentication factors affect security risk in relation to security costs by analyzing 55 two-factor authentication studies from ABI/Inform and EBSCOhost. It has been argued for many years that two-factor authentication can protect against the pitfalls of the password and PIN-only authentication system. However, there is no empirical evidence to support such an argument. Instead, I find that the research pattern of the two-factor authentication discipline has fallen into an undesirable "break-fix-break-fix" cycle. Much effort has been devoted, but little progress has been made. I also find strong evidence that many new proposed two-factor authentication schema can bring many unexpected risks. For future research, this study indicates that we need to increase the number, the quality of studies, and the critical stance of research on two-factor authentication.

Chapter 4 explores the tension of sustaining a decentralized digital resource system that retains high degrees of freedom to participate without creating incentives for free-riding. This was conducted through a four-year ethnographic study of one of China's largest online communities. Open digital resource systems become more valuable as accessibility (Hess & Ostrom, 2007) and community size (Butler, 2001) increase. However, this increase also creates the conditions for free-riding problems to arise (Olson, 1971). The existing online community literature defines free-riding based solely on whether the benefited users deliver the digital content forward for others to appropriate (Adar & Huberman, 2000; Baldwin & Clark, 2006; Mindel et al., 2018; Wasko et al., 2004). In contrast, this essay suggests that appropriating a digital resource without providing is not free-riding. My findings suggest that whether a behavior is free-riding or not should therefore be determined by the state of affairs they bring about (Driver, 2012; Mingers & Walsham, 2010; Scheffler, 1982). Riding-for-free, in other words, does not equate with free-riding. If content appropriation does not increase the participation cost of others, then it should not be considered free-riding. In contrast, *untruthful* and *useless* content provision could be free-riding. In this study, I conclude that even though digital resources cannot be depleted, the digital resource system could be made unsustainable by the value of digital resource systems being diminished through online community stakeholders' interaction with IT when their self-interest interactions increase the cost of the future others' IT use.

In conclusion, by zooming in on the unanticipated negative consequences of digitalization in different information system contexts, this dissertation demonstrates how IT can be used and interpreted by users and developers beyond its original intent and could produce a diminishing effect that reduces information system sustainability. This dissertation aims to show that the socio-

technical problem cannot be solved only by using better technologies but requires the technologies and their users to work collaboratively to produce better system outcomes.

References:

Adar, E., & Huberman, B. (2000). Free Riding on Gnutella. *First Monday*, *5*. https://doi.org/10.5210/fm.v5i10.792

Baird, A., & Maruping, L. M. (2021). The Next Generation Of Research On Is Use: A Theoretical Framework Of Delegation To And From Agentic Is Artifacts [Article]. *MIS Quarterly*, *45*(1), 315-341. https://doi.org/10.25300/MISQ/2021/15882

Baldwin, C. Y., & Clark, K. B. (2006). The Architecture of Participation: Does Code Architecture Mitigate Free Riding in the Open Source Development Model? *Management Science*, *52*(7), 1116-1127. https://doi.org/10.1287/mnsc.1060.0546

Baskerville, R. L., & Land, F. (2004). Socially self-destructing Systems. *The Social Study of Information and Communication Technology*.

Baskerville, R. L., Myers, M. D., & Youngjin, Y. (2020). Digital First: The Ontological Reversal And New Challenges for Information Systems Research [Article]. *MIS Quarterly*, *44*(2), 509-523. https://doi.org/10.25300/MISQ/2020/14418

Bostrom, R. P., & Heinen, J. S. (1977a). MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory. *MIS Quarterly*, *1*(4), 11-28. https://doi.org/10.2307/249019

Bostrom, R. P., & Heinen, J. S. (1977b). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. *MIS Quarterly*, *1*(3), 17-32. https://doi.org/10.2307/248710

Burton-Jones, A., Stein, M.-K., & Mishra, A. (2017). MISQ Research Curation on IS Use Research Curation Team. *MIS Quarterly Research Curations*, *1*(1), 1-24.

Butler, B. S. (2001). Membership Size, Communication Activity, and Sustainability: A Resource-Based Model of Online Social Structures [Article]. *Information Systems Research*, *12*(4), 346.

Butler, B. S., & Gray, P. H. (2006). Reliability, Mindfulness, and Information Systems. *MIS Quarterly*, *30*(2), 211-224. https://doi.org/10.2307/25148728

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality–social, clinical, and health psychology. *Psychological Bulletin*, *92*(1), 111-135. https://doi.org/10.1037/0033-2909.92.1.111

Davis, G. B. (2000). Information Systems Conceptual Foundations: Looking Backward and Forward. In R. Baskerville, J. Stage, & J. I. DeGross (Eds.), *Organizational and Social Perspectives on Information Technology: IFIP TC8 WG8.2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology June 9–11, 2000, Aalborg, Denmark* (pp. 61-82). Springer US. https://doi.org/10.1007/978-0-387-35505-4_5

Davis, G. B., Lee, A. S., Nickles, K. R., Chatterjee, S., Hartung, R., & Wu, Y. (1992). Diagnosis of an information system failure: A framework and interpretive process. *Information & Management*, *23*(5), 293-318. https://doi.org/https://doi.org/10.1016/0378-7206(92)90059-O

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable [Article]. *Information Systems Research*, *3*(1), 60-95. https://doi.org/10.1287/isre.3.1.60

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update [Article]. *Journal of Management Information Systems*, *19*(4), 9-30. https://doi.org/10.1080/07421222.2003.11045748

Dewan, R., Jing, B., & Seidmann, A. (2000). Adoption of Internet-Based Product Customization and Pricing Strategies. *Journal of Management Information Systems*, *17*(2), 9-28.

Driver, J. (2012). *Consequentialism*. Routledge.

Grover, V., & Lyytinen, K. (2015). New state of play in information systems research: the push to the edges. *MIS Q.*, *39*(2), 271–296. https://doi.org/10.25300/misq/2015/39.2.01

Güth, W., Schmittberger, R., & Schwarze, B. (1982). An experimental analysis of ultimatum bargaining. *Journal of Economic Behavior & Organization*, *3*(4), 367-388. https://doi.org/https://doi.org/10.1016/0167-2681(82)90011-7

Hess, C., & Ostrom, E. (2007). *Understanding Knowledge As a Commons: From Theory to Practice* [Book]. The MIT Press.

Klein, H. K., & Hirschheim, R. (1985). Fundamental issues of decision support systems: A consequentialist perspective. *Decision Support Systems*, *1*(1), 5-23. https://doi.org/https://doi.org/10.1016/0167-9236(85)90194-0

Mindel, V., Mathiassen, L., & Rai, A. (2018). THE SUSTAINABILITY OF POLYCENTRIC INFORMATION COMMONS [Article]. *MIS Quarterly*, *42*(2), 607-A614. https://doi.org/10.25300/MISQ/2018/14015

Mingers, J., & Walsham, G. (2010). Toward Ethical Information Systems: The Contribution of Discourse Ethics. *MIS Quarterly*, *34*(4), 833-854. https://doi.org/10.2307/25750707

Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, *3*(3), 398-427. https://doi.org/10.1287/orsc.3.3.398

Recker, J., Lukyanenko, R., Jabbari, M., Samuel, B. M., & Castellanos, A. (2021). From Representation To Mediation: A New Agenda For Conceptual Modeling Research In A Digital World [Article]. *MIS Quarterly*, *45*(1), 269-300. https://doi.org/10.25300/MISQ/2021/16027

Scheffler, S. (1982). *The Rejection of Consequentialism: A Philosophical Investigation of the Considerations Underlying Rival Moral Conceptions* (Vol. Rev. ed) [Book]. OUP Premium.

Shore, J., Baek, J., & Dellarocas, C. (2018). Network structure and patterns of information diversity on twitter. *MIS Q.*, *42*(3), 849–872. https://doi.org/10.25300/misq/2018/14558

Smith, A. (1761). *The theory of moral sentiments* (2d ed.). Printed for A. Millar, A. Kincaid and J. Bell in Edinburgh.

Smith, A. (1786). *An inquiry into the nature and causes of the wealth of nations* (4th ed.). Printed for A. Strahan, and T. Cadell.

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research Commentary—Digital Infrastructures: The Missing IS Research Agenda. *Information Systems Research*, *21*(4), 748-759. https://doi.org/10.1287/isre.1100.0318

Turel, O., Serenko, A., & Giles, P. (2011). Integrating technology addiction and use: an empirical investigation of online auction users. *MIS Q.*, *35*(4), 1043–1062.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146. https://doi.org/10.1126/science.aap9559

Wasko, M. M., Faraj, S., & Teigland, R. (2004). Collective Action and Knowledge Contribution in Electronic Networks of Practice [Article]. *Journal of the Association for Information Systems*, *5*(11/12), 493-513.

Yoo, Y. (2010). Computing in Everyday Life: A Call for Research on Experiential Computing. *MIS Quarterly*, *34*(2), 213-231. https://doi.org/10.2307/20721425
Zahedi, F. (1987). Reliability of Information Systems Based on the Critical Success Factors - Formulation. *MIS Quarterly*, *11*(2), 187-203. https://doi.org/10.2307/249362

Chapter 2 Preface

Information security systems include the security technology, users, security policy, and risk management plan. As a responsible society, we assume that investing in information security technologies helps organizations improve security performance. However, such an assumption may not be true in the context of an information security system because its weakest point (user behavior) could determine the reliability of the entire information security system.

While we hope that implementing a new information security technology can help our organizational security system become more reliable, this study demonstrates that the presence of information security technologies may trigger individual users to make more risky decisions, introducing more vulnerabilities into the information security systems.

This study responds to the thesis theme by demonstrating the information security system weaknesses and failure point, which is caused by security technology-induced behavior that reduces the reliability of the information security system, causing less sustainable information security systems. In addition, this study aims to challenge the conventional wisdom by showing that information security technologies may not solve the social-technical issues embedded in information security systems alone.

Chapter 2. When security technologies backfire: the behavioral tradeoff between information system functionality and information system security

2.1 Introduction

As a responsible society, we assume that investing in information security technologies helps organizations improve security performance. The empirical evidence, however, appears to contradict this assumption. For example, the PWC industry security report shows that the average organizational information security budget increased by 40% in 2015 (PWC, 2014). This security investment apparently generated no or little effect on the number of security incidents and consequent financial losses. The 2015 PWC report shows that the average financial loss due to security incidents decreased by the end of 2015 by only 5%, while the total number of reported security incidents increased by over 38% (PWC, 2015). The intended security increase that this investment aimed to achieve appears to have backfired. Organizations continue to increase their information security investment while the number of security incidents continues to rise. What can explain this paradox?

It is well established in the information security literature that adopting more advanced information security technologies leads to a more secure system. It has, however, been shown that this relationship can break down, or an unintended effect can even be caused under certain conditions (Angst et al., 2017; Lee et al., 2016; Sen & Borle, 2015; Wolff, 2016). For example, when implementing multiple layers of information security technologies, an organization must fully understand selected technologies' weaknesses to achieve maximum protection of the technological solutions. When the weakness of some technologies can be mitigated by the strength of others (Tirenin & Faatz, 1999), multiple security technologies can bring complementary effects, leading to a more secure system (Kwon & Johnson, 2014). Under certain conditions, more is not always

better. The literature has shown the contradictory pattern of IT security investment increasing the risk of a data breach. For example, Sen and Borle (2015) analyzed a large dataset of security incidents between 2005 and 2012 in the United States. They found that there is a strong significant correlation between the number of security incidents and IT security investment by industry or state sector. The inter-breach time decreased between 2005 and 2012 by 5.11% for every USD 1 billion increase in annual IT security investment. The most frequent data breach security incidents were, however, due to lost, discarded, or stolen mobile devices, outsiders causing only 22% of security incidents.

The information security literature has, without doubt, provided many fruitful insights into IT security investment effectiveness upon security breaches. However, the potential interaction between technological protection and system user-created vulnerabilities is overlooked, eclipsing alternative explanations such as whether our cybersecurity technologies induce new weaknesses and new strengths.

This study empirically investigates the impact of information security technologies (e.g., a virtual private network and two-factor authentication) on individual security decision-making. In particular, I pay attention to how the change in the system's security environment, which is afforded by the presence of new security technology, influences the psychological evaluation of an individual's decision choices' outcomes. I propose the following research question to guide my study:

How could system users' rational security decisions endanger the reliability of information security systems? In other words, how can system user behavior condition the effects of information security technologies?

My proposed security decision-making model has the potential to provide a fresh theoretical perspective on explaining the relationship between security technology adoption and the risk-taking behavior of information system users. My research extends an existing theory (i.e., self-regulation theory) by identifying two information security decision-making context-specific constructs- expected utility of security action decision and expected utility of insecurity action decision. My research objectives are to create a baseline decision model that captures how system end-users evaluate the expected utility of two mutually exclusive security decision choices' and select the decision choice with a higher expected utility outcome, and how such evaluation could trigger different security behaviors.

This research contributes to the information security literature, especially given that recent security literature has pointed to a psychological tipping point that normally compliant employees choose to become non-compliant and vice versa (Chen et al., 2021). My model would explain this tipping point or inconsistency between the theoretically predicted security behavior and the actual security behavior as the consequences of ***utility optimization*** between two mutually exclusive security decisions' outcomes. I argue that the main cause for these paradoxical phenomena is that the many existing decision models only reflect the evaluation of unilateral decisions, omitting the evaluation of the corresponding alternative decision. By incorporating the psychological evaluation of two mutually exclusive security decisions, my proposed decision model has the potential to explain not only the information security paradox but also other paradoxical phenomena, such as the privacy paradox, in which an individual's privacy belief is inconsistent with their privacy behavior.

In the remainder of this paper, I provide an overview of Carver and Scheier's self-regulation theory and how I adapt it to my specific context of security decision-making under uncertainty. This is followed by the development of our hypotheses, a description of the experiments I conducted to

test these hypotheses, and the results obtained. Finally, I discuss the research's contributions and limitations.

2.2 Theoretical Background

2.2.1 Self-Regulation Theory

Carver & Scheier's self-regulation theory is a control theory that is grounded in cybernetic literature (Wiener, 1948). It is widely accepted as a general theoretical framework for understanding an individual's behavior in their endeavors to attain their goals (Edwards, 1992). The self-regulation theory posits that an individual's behavior is part of the self-regulated system. In this self-regulated system, behavior is the output of the system feedback control in which individuals continuously evaluate their intended actions against the system's reference value (Carver & Scheier, 1982, 1990). When individuals sensing that their intended actions may cause deviations from their reference value, it would trigger a negative feedback loop that leads them to adjust their behaviors to reduce the discrepancy.

The theory of self-regulation suggests that behavior can be understood through the concept of feedback control (Carver and Scheier 1982; Carver and Scheier 1990). The theoretical foundation of this concept can be traced back to cybernetics theory (Wiener, 1948), in which behavior is understood to be "*any change of an entity with respect to its surrounding" (Rosenblueth et al., 1943, p. 18)* and "*all purposeful behavior may be considered to require negative feedback"* (Rosenblueth et al., 1943, p. 19). The negative-feedback loop is, in Carver & Scheier's self-regulation theory, the basic unit of the feedback control process. "Negative" here does not signal wrong or inappropriate behavior but serves as an analog of a function "*to negate or reduce sensed deviation from a comparison value"* (Carver & Scheier, 1982, p. 112). The purpose of the negative

feedback loop is to configure behaviors that ensure that the individual continues to approach the system's reference value (Carver & Scheier, 1982, 1990).

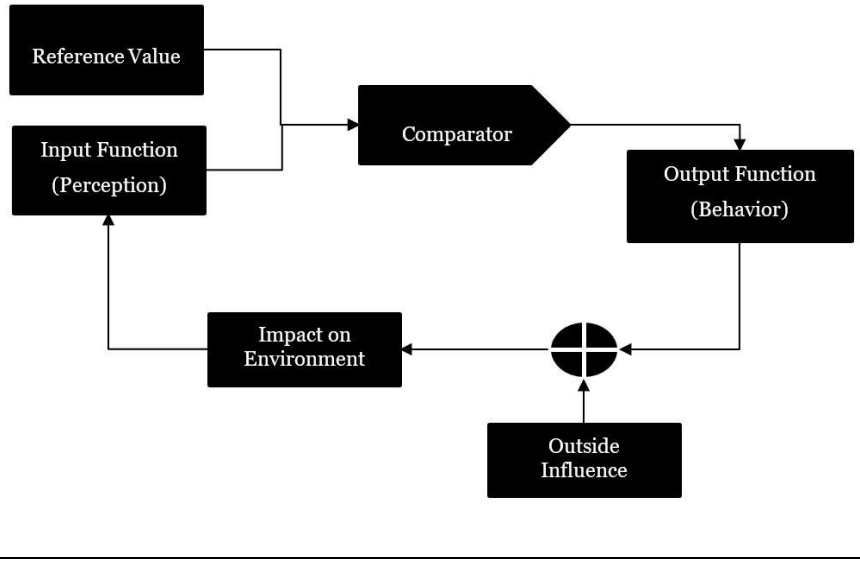

Figure 2-1. Negative Feedback Loop (adopted from Carver and Scheier 1990)

Negative feedback is a causal loop that consists of the input function, comparator, output function, reference value, environment, and disturbance factor (see Figure. 1). The input function is the individual's perception of their intended actions in the current state and is influenced by the environment. The comparator is the psychological evaluation that determines the discrepancy between intended actions in the current state and the system's reference value, the individual making modifications to their behaviors if a discrepancy between the two is detected, their programmed behaviors (e.g., routines) otherwise continuing. The result of the comparator will be sent to the output function, which is reflected in behaviors. Behavior, finally, does not directly create or minimize discrepancy but has an impact on the system environment. This is labeled *impact on the environment*. Such impact can change the current situation, leading to a new perception that serves as a new input to the next feedback loop. The disturbance factor, labeled

outside influence, can, however, be anything new from outside of the self-regulated system, which could impact the system environment and require individuals to configure their behavior to compensate for the changes and minimize discrepancies.

Purposeful behavior is always guided by goals (Rosenblueth et al., 1943; Wiener, 1948) or the reference value, as Carver and Scheier call this. The goals of self-regulated behavior are the three hierarchical level reference values (Carver & Scheier, 1990): system concept (e.g., be an idol), principle (e.g., be kind), and program (e.g., shovel snow off walks after snow). The highest reference value reflects the individual's *global sense of idealized self (i.e., system concept)*, the reference value at this level being abstract and difficult to define. Furthermore, this is the individual's lifetime goal, guiding their behavior and who they want to be. The next-level reference value is the *principle*, which reflects the individual's aspirations. The reference value at this level is also abstract but can be synthesized as personal qualities such as responsibility, honesty, and dignity. The lowest level reference value is the *program*. *Principle* influences *program* by determining what actions should be programmed and what decision choices should be made. Programs are individual, intended concrete activities being made up of sequences of movements of the decisions that must be made from choices (Carver & Scheier, 1990). Individuals do not, in practice, compare their daily actions with the complete hierarchy of reference values. Carver and Scheier (1990) suggest that feedback control tends to always exist at the program level, with little or no consideration of higher values until attention is redirected toward higher-level reference values. In this study, I investigate the reference value at the principle level. When the information systems' users are required to make immediate decisions facing security threats, they will evaluate the programed security decisions and select the decision according to their reference value. The programed decision and reference value is discussed in the next section.

Self-regulation theory provides an overarching framework for us to understand how the security environment change could potentially lead to behavioral configuration. In the following, I will discuss how the reference value from the self-regulation theory could be incorporated into security decision-making.

2.3 Hypothesis Development

Eisenhardt and Graebner (2007) suggest, for theory-driven research that extends an existing theory, that researchers must incorporate the theory within a specific context and explain how the theory would operate within that context. I draw the insights from the theory of self-regulation grounds in cybernetic literature and decision-making under uncertainty literature to provide an overarching framework to understand and analyze the interaction between system end-users security behavior and their information system security environment. In adopting the self-regulation theory to the context of security decision-making, I articulate that system users, behaviors, and the surrounding information system security environment works together as a self-regulated system. The perception by users of a change in the system's security environment due to new security technologies triggers the feedback loop that leads users to adjust their security behavior to compensate for the system environment change and to reduce the discrepancy according to the self-regulated system's reference value.

In the following section, I discuss how new information security technologies could trigger the feedback loop, cause behavioral re-configuration, and the minimization of the discrepancy between the system's environment and its reference value.

2.3.1 Reference Value at Principle Level

In this study, I articulate that, at the program level, programmed security decision choices generally can be classified into two mutually exclusive groups: security action decisions and insecurity action decisions. I define a ***security action decision*** as *the decision to expend energy by taking security action to increase system protection but decrease system functionality convenience,* and I define an ***insecurity action decision*** as the *decision to conserve energy by disregarding a security action in order to increase system functionality convenience but decrease system protection.* I argue that information system users who face security risk scenarios requiring an immediate decision choice generally tradeoff information system security with information system functionality convenience between mutually exclusive decisions.

The concept of *expected utility* is from the expected utility theory. The expected utility theory is the normative rational choice theory that describes how people should make decisions associated with uncertain outcomes (Savage, 1954; Von Neumann & Morgenstern, 1947). The expected utility theory posits that when individuals make a decision with uncertain outcomes, they will select the decision with the highest expected utility. Therefore, when evaluating two mutually exclusive security decisions, system users will evaluate and select the decisions according to the ***utility maximization***. In other words, I argue that the reference value in principle is the utility maximization in the context of the individual self-regulated decision.

Undoubtedly, the security literature offers many fruitful insights into individual decision choices under uncertainties. Many studies, however, tend to operationalize expected utility measurements for only one decision. They omit the alternative by implicitly assuming that the security action decision (e.g., no policy violation and response to security risk) and insecurity action decision (e.g., policy violation and no response to security risk) are at opposite ends of a single continuum.

However, a recent meta-analysis on security policy compliance and policy violation has indicated that policy compliance and policy violation do not appear to consistently measure opposite ends of the same behavior, as they share significant differences in antecedents (Cram et al., 2019). It is, therefore, reasonable to assume that an exogenous factor that increases the expected utility of a security action decision does not automatically increase the likelihood of users executing the security action. This is because the same exogenous factor may also increase the expected utility of the insecurity action decision. Therefore, to avoid inaccurate and unreliable results when examining exogenous factors' impact on decision choices, it is necessary to incorporate the evaluation of both security action and insecurity action decisions into the same decision model.

Indeed, to protect the system in a decentralized system environment, the system end-users need to make autonomous security decisions and appropriately interpret the current threat scenarios to pick the decision with the most desirable outcomes or highest expected utility. Specifically, when facing the security risk, system users evaluate the utility of the intended decision and the possible regret of the alternative outcomes associated with the same decision. That is, a decision, regardless of whether it is a security action decision or an insecurity action decision, could generate a positive outcome when it causes the user to experience *intended outcomes (i.e., security action decision for no security breach and insecurity action decision for system convenience)*, but the same decision choice could also generate negative outcome when it causes the users to experience unintended outcomes (i.e., security action decision for security breach and insecurity action decision for security breach.

2.3.2 IT protection to the Expected utility of security decisions

Savage (1954) proposes that individual subjective expected utility is the function of an individual's subjective utility and subjective probability distribution. I, thus, articulate that the expected utility

of security decisions is the function of individual system end-users perceived utility of the intended decisions and perceived probability of experiencing associated outcomes (i.e., no security breach for the intended security action decisions and security breach for the intended insecurity action decision). Since a security decision can only lead to two different states (i.e., security breach or no security breach), I, therefore, define the ***expected utility of a security action decision*** as *the function of the individual perceived utility of security breach and the perceived probability of experiencing no security breach given a security action*. I define the ***expected utility of an insecurity action decision*** as *the function of the individual perceived utility of the system functionality and the perceived probability of experiencing a breach given a no security action.*

I posit that information security technologies protection will be more likely to decrease the utility of security breach and increase the likelihood of no security breach occurrence with security actions, resulting in a decrease in the expected utility of security action decisions. Utility, within neoclassical economic literature, is the individual preference over a choice set (Savage, 1954; Von Neumann & Morgenstern, 1947). Although being referred to by different names, in the information security literature, utility is generally interpreted as the desirability of the behavioral outcomes associated with a particular security behavior. For example, much information security policy violation/compliance literature builds its arguments on the general deterrence theory (Chen et al., 2012; D'Arcy et al., 2009; Guo & Yuan, 2012; Straub & Welke, 1998), and the general argument that employees are less likely to execute insecurity practices (i.e., policy violations) when they perceive such actions to be less desirable due to the high sanction cost. The utility could similarly be the perceived appearance of the security threat. System users are more likely to execute security responses (e.g., comply with information security policy) that mitigate such

threats where the security threat appears to cause severe undesired outcomes (Herath & Rao, 2009; Johnston & Warkentin, 2010; Johnston et al., 2015).

The utility of the outcome is mostly measured by monetary value operationalized in the economic literature (e.g., Kahneman and Tversky (1979). However, the utility of a security decision is hard to measure by a ratio, causing difficulty in calculating the composite value of expected utility. Thus, instead of measuring the desirability of the states (i.e., security breach and no security bread) as the absolute magnitudes of final states (i.e., the desirability of the security breach and no security breach), I assume that the utility value carrier of a security decision choice is the degree of difference of utility between two states (Kahneman & Tversky, 1979). Therefore, individual users' perceived utility of breach could be best interpreted as their perceived severity of the breach.

In general, as information security technologies can generally make the security environment surrounding users safer, it is reasonable to believe that information security technologies can decrease the undesirable experience outcome (i.e., the utility of a security breach). For instance, an information system user can encrypt and save the encrypted data into a portable drive. Later, he may lose the portable drive. However, with the protection afforded by encryption technology, this may not eliminate a security breach but make the security breach less severe, decreasing the utility of a security breach compared with the situation of losing unencrypted data. In addition, if the same user exercises more security practices, such as never bringing the portable drive out of the company premise. The likelihood of no security breach will be further decreased with the help of his security practices. Therefore, the presence of security technologies should decrease the expected utility of security action decisions. I posit the following hypotheses.

H1. An increase in security technology's protection level will negatively influence system users' perceived utility of security action decisions.

Alternativity, the cybersecurity literature has shown that an organization's motivation to adopt IT security solutions can further break down the relationship between actual system security and security investment (Lee et al., 2016). IT investments in organizations that are motivated by a wish to reduce the legal liability of a data breach instead of achieving better system security may not improve the organization's system security. New or newly implemented security controls may, furthermore, have a negative impact on the operation and functionality of other preexisting security systems (Wolff, 2016) or trigger individual risk compensation (Zhang et al., 2009). This study would explain this unexpected relationship between the information security technology protection and actual system security as the consequences of increased expected utility of insecurity action decision. Information security technologies may increase the utility of system functionality. The utility of system functionality could include the availability or convenience afforded by the protected information systems. For instance, the Virtual Private Network (VPN) technology can allow the users to connect their computers outside the company premise when the internet connection is not secure. Thus, VPN technology increases availability and convenience for individual users to use their computers outside of the company premise, causing an increase in the utility of system functionality. In addition to that, with the extra protection, even though the users may exercise less security practices, the likelihood of security breach occurrence, thanks to the extra protection provided by the information security technologies, should be decreased. Therefore, the presence of information security technologies should increase the expected utility of insecurity action decisions. I posit the following hypothesis.

H2. An increase in security technology's protection level will positively influence system users' perceived utility of insecurity action decisions.

2.3.3 The expected utility of security decisions to security behavior

According to self-regulation, the feedback control process is relatively stable unless there is a disturbance (Carver & Scheier, 1990). According to self-regulation theory, the programmed decisions that the system users execute most of the time until the system security environment has been rechanged may require them to configure their behavior to reduce the discrepancy (Carver & Scheier, 1982, 1990). Similarly, presenting a new security technology into the context could cause the system security environment to change. Therefore, the system user would step outside the behavioral stream and re-evaluate the programmed decisions to see whether it is still the best choice.

According to self-regulation theory, the comparator's output is the behavior. The expected utility literature suggests that individuals are more likely to select the decision choices with the higher expected utility. Thus, systems users, when facing security threats with uncertain outcomes, would therefore execute the programmed decision choices (i.e., either security action decisions or insecurity action decisions) with the highest expected utility value. Therefore, I expect system users to be more likely to execute security action decisions when the expected utility of security action decisions is increased. In contrast, system users will be less likely to execute the security action decisions when the expected utility of an insecurity decision increases. Thus, I propose:

H3. The expected utility of security action decisions will positively influence system users' security action decisions.

H4. The expected utility of insecurity action decisions will negatively influence system users' security action decisions.

2.3.4 Mediation effects of expected utility of security decisions

Self-regulation theory indicates that two different feedback mechanisms can trigger the negative feedback loop (Carver & Scheier, 1990). The primary mechanism focuses on monitoring whether there is a discrepancy that needs to be rendered minimal. The secondary mechanism, however, emphasizes examining *"the rate of discrepancy reduction in the behavioral (monitoring) system over time"* (Carver & Scheier, 1990, p. 22). My research interest is to examine the impact of security technologies on the discrepancy between the expected utility value of the intended action and its alternative. I, therefore, in this study, focus on the negative feedback loop caused by the primary mechanism, the system user's dissatisfaction with their rate of approach to the reference value through intended actions being, however, beyond the scope of this study.

In the primary feedback mechanism, the self-regulation theory posits that system environment change is not, but comparator is, directly responsible for behavior. It also posits that the system environment only serves as the input to the comparator, the individual evaluating the current situation against the programmed actions based on the reference value at a higher level (Carver & Scheier, 1982, 1990). Therefore, the expected utility of a security/insecurity action decision will mediate the effect of security technology protection on the system user's actual security actions.

Even though the utility of a specific decision could be extremely high, an individual may still refuse to execute such a decision when they perceive that it is very unlikely that the decision will lead them to experience such utility. For example, information security policies may generate no deterrence effect where employees perceive that it is very unlikely they will be sanctioned for their policy violations (D'Arcy et al., 2009). System users will not respond to the security threat when the threat is unavoidable (Liang & Xue, 2009; Liang et al., 2019) or less likely to occur (Johnston et al., 2015), or when the intended security responses are unlikely to reduce the threat of occurrence

(Johnston & Warkentin, 2010). This study will explain the external factors that influence how individuals perceive different decision outcomes through two mechanisms. That is, increasing information security technology protection may increase the expected utility of insecurity action decisions. However, such utility change of insecurity action may not be larger than the decrease of expected utility of security decision. Thus, the users may still execute the security action decisions with the presence of information security technologies. Similarly, the lack of information security technologies may decrease the expected utility of insecurity action decisions. However, the expected utility of insecurity may still be larger than that of security action decisions. Thus, the users may still execute the insecurity action decision even though the system lacks security protection.

The increase in security technology protection will decrease the expected utility of security action decisions. Still, the increase in the utility of security action decisions will increase the likelihood of no breach occurrence given security action decisions. I, therefore, expect a negative mediating effect. Thus, I propose:

H5. The expected utility of security decisions will negatively mediate the influence of security technology protection on system users' security decisions.

I also expect a negative mediating effect of the expected utility of insecurity action decision between IT protection and security decision because the increase of security technology protection will increase the expected utility of insecurity action decisions. Still, a decrease in the expected utility of an insecurity action decision will decrease the likelihood of a security action decision. I, therefore, expect a negative mediating effect.

H6. The expected utility of insecurity decisions will negatively mediate the influence of security technology protection on system users' security decisions.

The theoretical security decision model is presented in figure 2. In the next section, I will discuss the methodology I used to test this model.

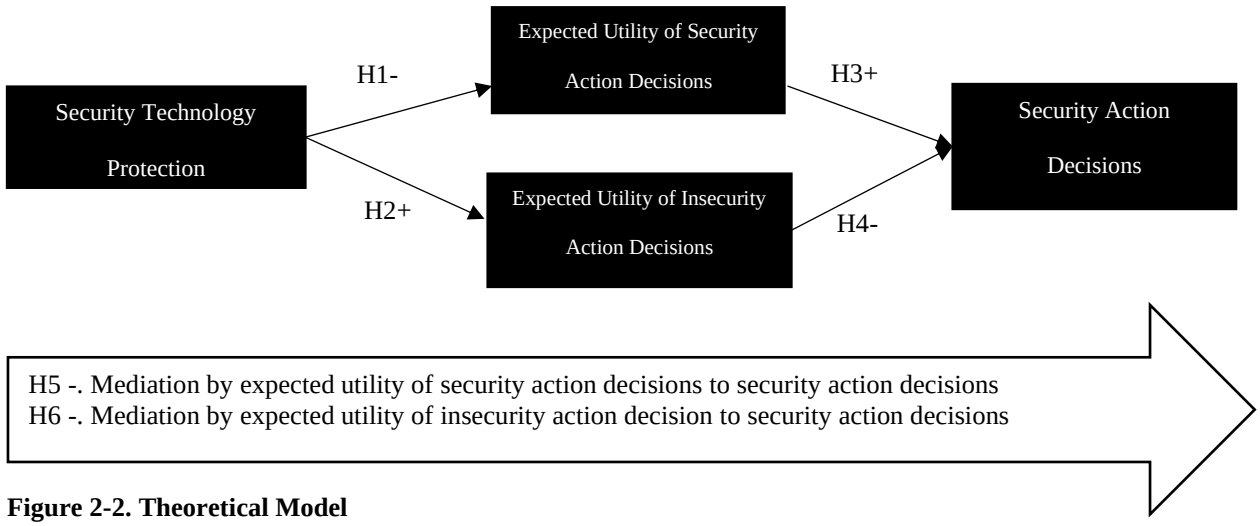

Figure 2-2. Theoretical Model

2.4 Research Methodology

2.4.1 Overview of Experiments

Given the nature of this study's hypothesis, a web-based experiment involving security threat scenarios was deemed the most appropriate. To test the hypothesis, I conducted a series of hypothetical scenario-based experiments to investigate the impact of security technologies on system users' expected utility of decisions and their security decisions. I selected the experimental method because our primary goal is to determine whether there is a causal relationship between security technology protection and security/insecurity action decision. One challenge of testing a new causal relationship between constructs is ensuring internal validity. A lab experiment is one of the most appropriate methods to achieve high internal validity (Lee et al., 2019).

A hypothetical scenario-based experiment is also a common approach in the information system literature on various topics (Johnston and Warkentin 2010; Johnston et al. 2015; Liang et al. 2019). Field studies are problematic due to the nature of the information security context, as companies may not allow their employees to release the security incidents or security breach-related information to third parties (Chen et al., 2012). Scenario-based experiments can offer us an indirect way of measuring participants' socially undesirable behaviors (Finch, 1987; Siponen & Vance, 2010). Scenario-based techniques furthermore allow researchers to examine the issue "in the way which approximates to the complexities with such issues are surrounded in reality (Finch, 1987, p. 111)". Scenario-based techniques offer an advantage by replicating or at least coming closer to the issue, ensuring the study's generalizability.

Table 2-1. Experiment Scenarios

Scenario	Sources
Failing to lock or log out of workstations	
You are an employee in the XYZ organization. You have been given authorized access to the company's payroll system as part of your job. One day at work, you log into the payroll system to gather information for a weekly report that you prepare for your management team. During the middle of work, you are in need of a short restroom break. Finding it is convenient to keep the system logged in, will you keep your workstation logged in during the short restroom break?	Adapted from Siponen and Vance (2010), D'Arcy et al. (2014), Moody et al. (2018)
Creating a simple password	
You are an employee in the XYZ organization. The organization recently installed a computer system for managing employee personal information (e.g., employee emergency contacts, retirement benefits, salary information). Each employee is required to set up a user account to access the system. If you find it difficult to remember the password, will you create a simple password or a complex one? *(Note: we changed the question from writing down the password in the prior literature to creating a simple password or a complex password)*	Adapted from Guo and Yuan (2012), D'Arcy et al. (2014), Guo et al. (2011)
Sharing passwords with colleagues	
You are an employee in the XYZ organization. You are on a business trip, and one of your coworkers needs a file on your computer.	Adapted from Siponen and Vance (2010),

You expect that sharing your password could save your coworker time and effort. Will you share your password with your coworker?	D'Arcy et al. (2014), Vance et al. (2014)
Copying corporate data to insecure USB	
You are an employee in the XYZ organization. You are currently working on a sales report that requires analyzing the company's customer database, which contains sensitive financial and purchase history information. Next week, you will travel for several days and would like to analyze the corporate data on the road. You expect that analyzing your company data during the trip can save your company a lot of time. Will you copy the company's data to a portable drive?	Adapted from Siponen and Vance (2010), Moody et al. (2018), D'Arcy et al. (2014), Guo et al. (2011), Vance et al. (2012)
Using laptops carelessly outside of the company	
You are an employee in the XYZ organization. You use a corporate laptop while traveling to other sites or working from home. You often bring the laptop to do some work when having a coffee at coffee shops. As you know, many coffee shops nowadays offer free and password-free Wi-Fi. At this time, you need an internet connection to download an important document emailed from your coworker. Will you connect your corporate laptop to the coffee shop Wi-Fi?	Adapted from Guo and Yuan (2012), Guo et al. (2011)

2.4.2 Experimental procedure

I adopted the scenarios from the information security literature to ensure that my choice of threat scenarios was relevant and realistic to practice. I synthesized those scenarios into categories following Siponen and Vance (2010). After removing the manipulations that used in the existing studies, the selected threat scenarios can be classified into the five most frequent security threat categories according to Siponen and Vance (2010): The five categories include failing to lock or log out of workstations, creating a simple password, sharing passwords with colleagues, copying corporate data to a portable drive, and using laptops carelessly outside of the company. In addition, I also measured the realistic score for each individual scenario (D'Arcy et al., 2014; Moody et al., 2018). I asked participants to rate each scenario's realism (1 = "highly unrealistic" to 7 = "high realistic") and I used this measure as additional control variables in the analysis. The mean realism score for each scenario is 5.5 out of 7, which provide reasonable assurances that the scenarios were realistic and acceptable by the existing information security literature.

Table 2-2. Manipulation Design	
High-security protection	**Low-security protection**
Failing to lock or log out of workstations	
At this time, your company recently adopted an information security system that uses an embedded camera to monitor active users' faces continuously. If the security system detects an unauthorized user, the security system would automatically lock down the workstation. At this time, when you need a short restroom break, what would you do?	Currently, your company's information security system has some technical issues. In the past, the information security system used an embedded camera to continuously monitors active users' faces. If the security system detects an unauthorized user, the security system would automatically lock the workstation. However, the security system is no longer working. At this time, when you need a short restroom break, what would you do?
Creating a simple password	
Your company recently adopted a two-factor authentication system that requires both passwords and a one-time-use SMS passcode to log into the system for all employees' accounts. At this time, when you need to create a new password, what would you do?	Your company's two-factor authentication system has some technical issues. In the past, the security system requires both a password and a one-time-use SMS passcode to log into the system for all employees" accounts. However, due to the information security systems issues, your company has to disable the two-factor authentication system. At this time, when you need to create a new password, what would you do?
Sharing passwords with colleagues	
Your company recently adopted an information security system that allows you to generate a one-time password. At this time, when your coworker needs to access your computer, would you share your one-time password with your coworker?	You try to use your company's recently adopted information security system to generate a one-time passcode to share with your coworker. However, the security system has some technical issues and stopped working. At this time, when your coworker needs to access your computer, would you share your password with your coworker?
Copying corporate data to insecure USB	
You discover that your company recently adopted security software to create a password to encrypt the data. At this time, when your need to analyze the company's data on the road, would you copy the company's encrypted data to a portable drive?	You try to use your company's recently adopted information security software to encrypt the corporate data. However, you find the security software has some technical issues that no longer allow you to encrypt the data. At this time, when you need to analyze the company's data on the road, would you copy the company's data to a portable drive?
Using laptops carelessly outside of the company	
Your company adopted VPN software that can encrypt the network connection between your laptop and the company's data server.	Your company adopted VPN software that can encrypt the network connection between your laptop and the company's data server. However, when you try to start the

At this time, when you need the internet at the coffee shop, would you connect your laptop to the public Wi-Fi with the VPN?	VPN software, you find the system has some technical issues that the VPN is no longer working. At this time, when you need internet at the coffee shop, would you connect your laptop to the public Wi-Fi without the VPN?

I first run a pilot to examine whether the presence of information security technology can influence security decision-making. Participants in the pilot study were randomly assigned to two conditions: high-security technology protection and low-security technology protection (see Table 2.). Each participant read all five threat scenarios. I manipulated the objective level of protection by providing additional information on the individuals' system security environment. Participants in the high level of security technology protection condition were told that the company had recently adopted a security technology that can be used to mitigate the risks of the assigned scenarios.

In contrast, participants in the low-security technology protection condition were told that the recently adopted security technology is malfunctioning and no longer provides security protection. I selected security technologies in the scenarios that can mitigate risks by consulting two experts in information security risk management and referring to the NIST security control catalog (2012). After reading each scenario, participants were asked to select their decision choice, either security action or insecurity action decision. The manipulations check was performed, showing a significant difference in the perceived level of security protection between the two groups in both the pilot and final experiment.

In the pilot study, I recruited about 200 participants from Amazon MTurk. The result supported our initial assumption that the presence of information security indeed decreases the likelihood of security action decisions ($p<0.001$).

Table 2-3. Measurements		
Variable	**Measurement**	**Adapted From**
Perceived Utility of System Functionality	***High-Protection Condition*** *1. Information security technology that actually works well can help me save time.* *2. Information security technology that actually works well can help me increase my work productivity.* *3. Information security technology that actually works well can increase my computer system's availability.* *4. Information security technology that actually works well can increase the convenience afforded by my computer system.*	(Boss et al., 2015; Woon et al., 2005)
	Low-Protection Condition *1. Information security technology that actually works poorly can help me save time.* *2. Information security technology that actually works poorly can help me increase my work productivity.* *3. Information security technology that actually works poorly can increase my computer system's functionality or availability.* *4. Information security technology that actually works poorly can increase the convenience afforded by my computer system.*	
Perceived Probability of Breach Occurrence Given No Security Action	***High-Protection Condition*** *1. When Information security technology actually works well, I would become a victim of an information security threat if I make an unsafe security decision.* *2. When Information security technology actually works well, my organization would become a victim of an information security threat if I make an unsafe security decision.* *3. When Information security technology actually works well, an information security threat would occur if I make an unsafe security decision.*	(Boss et al., 2015; Guo et al., 2011)
	Low-Protection Condition *1. When Information security technology actually works poorly, I would become a victim of an information security threat if I make an unsafe security decision.* *2. When Information security technology actually works poorly, my organization would become a victim of an information security threat if I make an unsafe security decision.* *3. When Information security technology actually works poorly, an information security threat would occur if I make an unsafe security decision.*	
Perceived Utility of Breach	***High-Protection Condition*** *1. Information security technology that actually works well can increase the seriousness of an information security breach to me.* *2. Information security technology that actually works well can increase the seriousness of an information security breach in my organization.* *3. Information security technology that actually works well can increase the severity of an information security breach.*	(Johnston & Warkentin, 2010; Milne et al., 2000)

	4. Information security technology that actually works well can increase the seriousness of an information security threat. *5. Information security technology that actually works well can increase the significance of an information security breach.*	
	Low-Protection Condition *1. Information security technology that actually works poorly can increase the seriousness of an information security breach to me.* *2. Information security technology that actually works poorly can increase the seriousness of an information security breach in my organization.* *3. Information security technology that actually works poorly can increase the severity of an information security breach.* *4. Information security technology that actually works poorly can increase the seriousness of an information security threat.* *5. Information security technology that actually works poorly can increase the significance of an information security breach.*	
Perceived Probability of No Breach Occurrence Given Security Action	***High-Protection Condition*** *1. When Information security technology actually works well, I would not become a victim of an information security threat if I make a safe security decision.* *2. When Information security technology actually works well, my organization would not become a victim of an information security threat if I make a safe security decision.* *3. When Information security technology actually works well, an information security threat would not occur if I make a safe security decision.*	(Boss et al., 2015; Guo et al., 2011)
	Low-Protection Condition *1. When Information security technology actually works poorly, I would not become a victim of an information security threat if I make a safe security decision.* *2. When Information security technology actually works poorly, my organization would not become a victim of an information security threat if I make a safe security decision.* *3. When Information security technology actually works poorly, an information security threat would not occur if I make a safe security decision.*	

In the final experiment, there are two major differences between our pilot experiment and the final experiment. First, the mediators' questions were added to the scenarios in the final experiment. From the existing literature, I adapted the measurement items for the utility of security breach, the

utility of system functionality, the perceived probability of no breach occurrence with security action, and breach occurrence with no security action. The actual measurement items for each individual construct are shown in Table 3. Second, I randomly assigned the participant to one thread scenario instead of five scenarios in the pilot study, the threat scenario. By doing this, it will increase the internal validity due to less likelihood of learning effect or scenario ordering effect.

In the final study, I recruited about 500 participants from Prolific.co, and the details of our final dataset are discussed in the data analysis section. Recruiting participants from a different platform can help me increase the external validity and prevent the participants from taking the experiment more than once.

2.4.3 Measurement model development

For the outcome variable, I measured individual decisions instead of decision intention. Cram et al. (2019) suggest that examining security behavior is more fruitful because intention may not always lead to security behaviors. Cram et al. conducted a meta-analysis and found that employees' intentions to comply with the policy differ from actual compliance behavior, where response cost is considered. Cram et al. (2019) speculate that employees tend to underestimate the burden cost (or response cost) when considering compliance. However, such burden cost (or response cost) negatively impacts their actual compliance. I, therefore, used hypothetical decision-making choices (i.e., make a security action decision or make an insecurity action decision) as the dependent variable for measuring system users' security behaviors that were used by the previous study (Liang et al., 2019).

Bergkvist and Rossiter (2007) suggest that the single-item measure can provide the same predictive validity as the multiple-item measure. The multiple-item measure is required where the construct is abstract and the object of the construct comprises two or more components. The single-item

should otherwise be used because the multiple-item can increase the research cost or even bring about the risk of harming research quality (e.g., self-generated validity) (Bergkvist, 2015; Bergkvist & Rossiter, 2007). The outcome variable, which is security decisions), used a single-item measure. This fits Bergkvist and Rossiter (2007)'s criteria for the single-item measure while retaining sufficient predictive validity.

I operationalize the mediators as reflective-and-formative second-order constructs. The first-order constructs, including the utility of security breach, the utility of system functionality, probability of no breach occurrence given security action, and probability of breach occurrence given insecurity action, were operationalized as a reflective construct (see Table 3). For the second order, constructs, which are expected utility of security action decision and expected utility of insecurity action decision, were operationalized as formative constructs. For the first-order construct, I adapted measurement items from the existing security literature (see Table 3).

It is worth noting that the perceived probability of breach occurrence and no occurrence were operationalized as the conditional probability of associated security outcomes given different security decisions. The purposes of measuring the perceived conditional probability of different security outcomes given different decisions are to increase discriminant validity and reduce the ambiguity of the survey questions. The challenge of measuring the probability part of expected utility is that security decision choices (i.e., act) and security outcomes (i.e., state) are not probabilistically and logically independent. When the states are probabilistically independent of acts, the conditional probability of states, given that one of the acts is done, will be equal to the unconditional probability of the states (Nozick, 1969). For instance, a user security action decision can, to a certain degree, be effective in alleviating the likelihood of a security threat, and the perceived likelihood of the breach, meanwhile, will influence the likelihood of executing the

security response (Johnston & Warkentin, 2010; Johnston et al., 2015; Liang & Xue, 2009; Liang et al., 2019), causing different expected utility of security action decision if the user intends to exercise an insecurity action decision. Therefore, it is necessary to measure the probability part of expected utility theory by using the conditional probability (statement) instead of ambiguous, unconditional probability belief.

I operationalized the mediators as reflective-and-formative second-order constructs for the following reasons. First, whether the construct is reflective and formative should rest on the theoretical consideration (Petter et al., 2007). The primary difference between the reflective construct and formative construct is that while the change of reflective indicators causes the variance of the reflective construct, the direction of causality is reversed in the formative construct that the change of formative construct (Cenfetelli & Bassellier, 2009). The expected utility theory indicates that the expected utility of a decision is the function of the state's perceived probability and the state's perceived utility. Thus, the causal direction is from the utility and probability to the expected utility of a decision. In other words, the expected utility of a decision should be increased with the increase in the perceived probability of the state and the perceived utility of the state. In contrast, the increase in the expected utility of a decision does not warrant the increase in the perceived utility of a state or the increase in the perceived probability of a state occurrence. Second, the lower order constructs (i.e., utility and probability) are theoretically independent. While multicollinearity is desired among measures for reflective constructs, it may cause a problem for formative constructs (Petter et al., 2007). In other words, the increase in the perceived probability of a state occurrence has no direct impact on the perceived utility of a state and vice versa. For instance, purchasing a lottery can be considered decision-making under the risk. Purchasing multiple lottery tickets can increase the perceived probability of winning a jackpot. However, such

an increase in the number of lottery tickets should have little or no effect on the individual's perceived utility of winning a jackpot. Still, it does increase the overall expected utility of such a decision. Third, I operationalized the expected utility of security decision as a higher order formative constructs because such bundling of lower order construct could enhance parsimony through the substitution of a single construct (Cenfetelli & Bassellier, 2009), so the formative constructs allow us to focus attention on a single construal effect as opposed to multiple observable indicator effects. Thus, operationalizing the expected utility of security decisions as a reflective-and-formative second-order construct can help us avoid statistical conclusion errors that can occur from specifying the measurement model(Petter et al., 2007). The following section will discuss the measurement model validation procedure and results.

2.4.4 Measurement model validation

Partial least square (PLS) was used for the data analysis. This analytical approach is recommended for research models with an emphasis on theory development (Rai et al., 2006). Also, PLS employs a component-based approach for estimation, a recommended analytical approach for handling formative constructs (Chin, 1998).

To avoid misinterpreting the formative constructs validation results, I followed Cenfetelli and Bassellier (2009)'s suggestions on the potential five issues that may arise when employing formative measures. The five issues are (1) multicollinearity among the indicators, (2) number of indicators and nonsignificant weight, (3) co-occurrence of negative and positive indicator weights, (4) absolute versus relative indicator contribution, and (5) nomological network effect.

(1) Multicollinearity

Cenfetelli and Bassellier (2009) suggest that one issue with the formative measure is when indicator weights have very different results in magnitude, sign, and significance caused by multicollinearity. To address the potential multicollinearity issues, I performed a factor analysis by using SmartPLS 3.0. The recommended variance inflation factor (VIF) is below 3.33 (Diamantopoulos, 2006) or 10 (Hair, 2006). The PLS factory analysis results show that the VIF value perceived utility of breach, perceived utility of system functionality, the perceived probability of no breach occurrence given security action, and perceived probability of breach occurrence given no security action is below the threshold of 3.33 (See table 4 for VIF results). Thus, the formative constructs have no potential multicollinearity problem.

Table 2-4. PLS Inner VIF Value Matrix

	Expected Utility of Security Action Decision	Expected Utility of Insecurity Action Decision
Perceived utility of breach	1.621	
Perceived probability of no breach occurrence given security action	1.418	
Perceived utility of system functionality	-	2.182
Perceived probability of breach occurrence given no security action	-	1.284

Table 2-5. Indicator Weights and Significance

	Path	T-test	P value
Perceived utility of breach	- 0.335	24.114	0.000
Perceived probability of no breach occurrence given security action	0.821	44.291	0.000
Perceived utility of system functionality	0.771	36.051	0.000
perceived probability of breach occurrence given no security action	-0.482	7.843	0.000
Bootstrap based on 5,000 at 5% two-tailed significant level			

(2) Number of indicators specified for a formatively measured construct

To test issue 2, Cenfetelli and Bassellier (2009) suggest the researcher keep all indicators forming a single construct to test whether the indicators have significant paths to the formative construct. The PLS results show that all the indicators have a significant path coefficient to their formative construct. Thus, issue 2 has been addressed.

(3) Co-occurrence of Negative and Positive Indicator Weights

Cenfetelli and Bassellier (2009) suggest that a possible co-occurrence of both positive and negative indicator weight may occur when validating the formative construct. When both positive and negative weight exists in the formative construct, the researcher should exercise caution when interpreting the result and not remove them if they are significant. The PLS results show that I do have co-occurrence of both positive and negative indicator weight in our formative constructs. However, this co-occurrence of positive and negative indicators aligns with the theoretical assumption. For instance, when the perceived utility of breach remains constant, the increased amount of perceived probability of no breach occurrence given action will reduce the degree of expected utility of security action decision. In other words, when the security practices can effectively reduce the likelihood of breach occurrence, even though the breach consequence could be less severe, the users will believe that the execution of security practices is necessary. Thus, issue 3 has been addressed.

(4) Absolute versus relative indicator contributions

Cenfetelli and Bassellier (2009) suggest it is necessary to discuss formative indicator weights to determine their relative contribution to their assigned constructs. The PLS result shows that the total effect with the expected utility of security action is 0.821 and -0.335 for the perceived utility of breach and perceived probability of no breach occurrence given action, respectively. In addition,

the PLS result shows a total effect with the expected utility of insecurity action of 0.711 and -0.482 for the perceived utility of system functionality and perceived probability of breach occurrence given no security action, respectively. And they are significant from zero. All of the indicators' paths to their assigned formative constructs are significant from zero. This suggests that each of those indicators has a strong bivariate relationship with the expected utility of security action and with the expected utility of insecurity action decisions.

(5) Nomological Network Effects

Cenfetelli and Bassellier (2009) suggest that "*the relative invariance of construct's indicator weights as the constructs used in the construct is used in different nomological networks* (p.698)." In an ideal situation, the weights of the indicators for its assigned formative construct should not be changed much when adding a new construct to the measurement model. To test the potential nomological network effects, I added all control variables (i.e., demographic info and Scenarios (as categorical)) and outcome variables into the measurement model. I did not observe a significant change in the scale of indicators weight when added new constructs for both formative measurements. Thus, the nomological network effect should not cause potential issues for the formative measurement.

Table 2-6. Reflective Measurement Model Validation

Construct Indicator	Factor Loading	Cronbach's Alpha	Composite Reliability	Average Variance Extracted
Utility of Breach		0.970 (240.194 ***)	0.977 (317.895***)	0.893 (69.771 ***)
UoB1	0.935 (73.281***)			
UoB2	0.958 (137.169***)			
UoB3	0.950 (121.276***)			
UoB4	0.944 (86.562***)			
UoB5	0.939 (92.744***)			

Probability of No Breach Given Action		0.934 (104.703***)	0.958 (176.337***)	0.833 (63.981***)
No_Brech_Act1	0.919 (65.996***)			
No_Brech_Act2	0.961 (163.490***)			
No_Brech_Act3	0.939 (117.232***)			
Utility of System Functionality		0.944 (174.928 ***)	0.960 (259.660***)	0.856 (73.136 ***)
UoF1	0.941 (157.445***)			
UoF2	0.943 (156.023***)			
UoF3	0.890 (60.308***)			
UoF4	0.926 (91.691***)			
Probability of Breach Given No Action		0.955 (158.281***)	0.971 (256.532***)	0.918 (90.747***)
Brech_No_Act1	0.957 (7.919***)			
Brech_No_Act2	0.963 (7.916***)			
Brech_No_Act3	0.953 (7.913***)			
*p < .05, **p < .01, ***p < .001				

I operationalized the lower-order constructs as reflective measurements. To evaluate the validity of our reflective measurement, I performed a factor analysis for the measurement model. All the factor loadings are greater or closer to 0.90 and exhibit an acceptable quality of item reliability (see Table 6). Convergent validity can be examined in terms of the reliability of constructs (i.e., Cronbach's Alpha), the composite reliability of constructs, and the average variance extracted by constructs. Cronbach's alpha over 0.9 indicates good construct reliability. The PLS results show that all the reflective constructs have Cronbach's alpha value over 0.9. Also, the composite reliability of constructs can measure the internal consistency. A value above 0.7 indicates an acceptable internal consistency. PLS results show that all the reflective constructs have a composite reliability value over 0.9, which indicates that the reflective constructs have achieved a

good internal consistency. Last, the value of the average variance extracted by the indicators is all above the 0.8 level, indicating the variance captured by our indicators is much greater than the measurement errors.

To conclude, The measurement validation analysis results indicate that I achieve a sufficient level of item reliability, and construct convergent and discriminant validity. In the following, I will discuss our hypotheses testing results.

2.4.5 Structural Model Analysis Results

In the final experiment, I manipulated the between-subjects effect of security technology by changing the objective level of security technology protection. A total of 579 participants from Prolific.co completed the study, each being paid $1.00. I recruited workers who speak English as the first language, work part-time or full-time, and use information technology at least once per week. The average participant completed the study in about 5 to 6 minutes. The final dataset contained 461 valid observations (see Table 7 for detailed demographic info and assigned scenarios) after filtering for participants who failed the attention checks and completed the survey in an unusually short space of time (i.e., under 2 minutes) and who made multiple entrances to the study and has the fraudulent score over 10 (out of 100).

Table 7. Participants Demographic info and Assigned Scenario Frequency Table

	Frequency	**Percentage**
Gender		
Male	242	52.5%
Female	219	47.5%
Age		
Under 18	0	0%
18 to 30	116	25.2%
31 to 40	160	34.7%
41 to 50	77	16.7%
51 to 60	79	17.1%
61 to 70	26	5.6%
71 and above	3	0.7%
Education		

Less than high school	4	0.9%
High School	152	33%
Bachelor's degree	222	48.2%
Master's degree	73	15.8%
PhD	10	2.2%
Work Experience		
Under 1 year	3	0.7%
1 to 3 years	26	5.4%
3 to 5 years	22	4.8%
5 to 8 years	44	9.5%
8 years and above	367	79.6%
Assigned Scenario		
Login Workstation	90	19.5%
Simple Password	92	20%
Sharing Password	96	20.8%
Portable Drive	93	20.2%
Public Wi-Fi	90	19.5%

I first performed an ANOVA analysis to check whether our manipulation caused significant differences between the low-technology protection group (Mean = 2.393, Std = 0.829) and the high-technology protection group (Mean= 5.732, Std =0.664). The results show a significant mean difference between the two groups regarding the perceived level of protection ($F = 2298.752$, $p < 0.001$).

I tested the structural model using SmartPLS 3.0; the results are shown in Figure 3. The control variables are Gender, Age, education, work experience, and scenario number (categorical dummy variable). The exogenous variable (X) is the Level of Security Technology Protection (1 = low-security protection, 2 = high-security protection); the mediators are *Expected Utility of Security Action Decisions* and *Expected Utility of Insecurity Decisions*; the dependent variable is *Security Action Decisions* (1= insecurity action decision, 2 = security action decision). The PLS results indicate that our structural model has a good model fit (SRMR = 0.004, d ULS = 0.002, Chi-Square =2.919, NFI = 0.998).

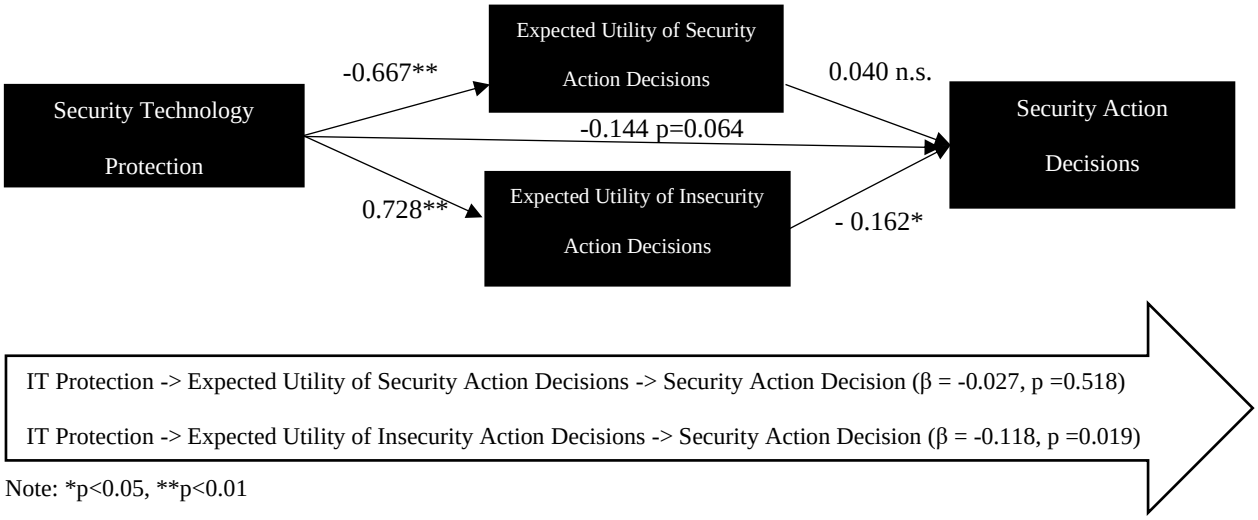

Figure 2-3. Theoretical Model

In PLS, higher order factors can be approximated by using repeated indicators following Lohmoller (1988) hierarchical component model (Chin et al., 2003). Lohmoller (1988) hierarchical component model directly measures the high-order constructs using all items of its lower-order construct. To do this, I followed the steps suggested by Lowry and Gaskin (2014). I created second-order constructs for the expected utility of security action decisions and expected utility of insecurity actions that contain all its assigned indicators in the first-order constructs. However, Lowry and Gaskin (2014) pointed out that this repeated indicator approach works well when the second-order constructs are reflective. When the second-order constructs are formative and endogenous, the repeated indicators in the second-order construct are perfectly predicted by the first-order constructs. To overcome these issues, I followed Lowry and Gaskin (2014) recommended two-step approach. I first modeled the measurement model and obtained the laten

Table 2-8. Results of PLS Analyses by using Two-Step Approach			
Variables	**U. of Security Action**	**U. of insecurity Action**	**Security Decisions**
Controls			
Gender	0.042	-0.034	-0.083
Age	-0.032	-0.020	-0.036
Education	-0.019	0.030	-0.029
Work Experience	-0.019	-0.017	0.067
S1-Login Workstation	0.055	0.051	0.189***
S2- Simple Password	0.015	0.044	0.028
S3- Sharing Password	0.064	-0.013	0.042
S4- Data Encryption	0.020	0.009	0.051
S5- Public Wi-Fi	-	-	-
Predictors			
Security Technology (H1 & H2)	-0.667***	0.728***	-0.144 (p = 0.064)
U. of Security Action* (H3)			0.040 (p=0.517)
U. of insecurity Action* (H4)			-0.162* (p=0.018)
R^2	0.448	0.543	0.141
R^2 $Adjusted$	0.437	0.534	0.120

1. PLS results are based on 5,000 Bootstrap samples at a 5% two-tailed significant level
2. Sample size n = 461, Gender is dummy coded (1= Men, 2= Women); Security Decision is dummy coded (1 =Insecurity action, 2= security action); Security Technology is dummy code (1= low security technology protection, 2 = high security technology protection), Scenario number are categorical and coded as dummy variable (0 = Not Assigned, 1 = Assigned)
3. *p < .05, **p < .01, ***p < .001

variable score for the expected utility of security action decisions and expected utility of insecurity action decisions. After that, we create a new model that uses the latent variable score as indicators of the second-order constructs (i.e., the expected utility of security action decisions and insecurity action decisions) and IT protection, security action decisions, and control variables. The detailed path coefficients are shown in table 8.

As the results in Table 8 show, the decision model explained 14.1 % of the total variance of individual actual security decision choices after adding our control variables to the model. In H1, I posit that security technology protection would negatively affect system users' expected utility

of security action decisions. The coefficient for security technology protection is negative and significant in its prediction (β = -0.667, p <0.001), so H1 is supported. In H2, I posit that security technology protection would positively affect system user expected utility of insecurity action decisions. The coefficient for security technology protection is positive and significant in prediction (β = 0.728, p <.001), which is consistent with this hypothesis. Thus, H2 is supported. In H3, I posit that the expected utility of the security action decision has a positive relationship with the security action decision. The coefficient for this path is positive but not significant (β = 0.040, p =0.517), so I fail to support H3. Last, I posit that the expected utility of the insecurity action decision has a negative relationship with the security action decision. The coefficient is negative and significant (β = 0.040, p =0.018), so H4 is supported.

For the mediation effect, I estimated the indirect effect using 5,000 bootstrap samples as advocated (Hayes, 2018). PLS bootstrapping has many advantages. First, the multiple mediators model allows us to estimate direct and indirect effects while accounting for covariance between constructs. Second, PLS bootstrapping allows researchers to perform bootstrapping without requiring a large sample. Third, the mediation estimated tends to have a skewed sampling distribution because it involves the product of terms (Maruping & Magni, 2015). The confident interval (CI) produced by bootstrapping is robust to this challenge (Wood et al., 2008). The mediation analysis results are presented in Table 9.

Table 9. Results of Mediation Analysis

			Bias corrected 95% CI	
Constructs	**Effect**	**Bias**	**Lower**	**Upper**
	Total effect of Security Technology on Decision			
	-0.289	0.000	-0.374	-0.204
	Direct effect of Security Technology on Decision			
Security Technology Protection	-0.144	0.002	-0.297	0.010
	Indirect effect of Security Technology on Decision			

U of Security Action	-0.027	-0.001	-0.108	0.059
U of Insecurity Action	-0.118	-0.001	-0.214	-0.018

H5 states that the expected utility of security decisions will negatively mediate the influence of security technology protection on individual security decisions. As the results in Table 9 show, the indirect effect of security technology protection on security action decisions through the expected utility of security actions is negative but not significant (indirect effect: -0.027, 95% CI: -0.108 to 0.059). H5 is therefore not supported. H6 state that the expected utility of insecurity decisions will negatively mediate the influence of security technology protection on individual security decisions. The result shows that the indirect effect of security technology protection on security action decisions, through the expected utility of insecurity action, is negative and significant (indirect effect: -0.1118, 95% CI: -0.214 to -0.018). H6 is therefore supported.

In addition, the mediation analysis also shows that information security technology protection has a negative but not significant correlation with security action decisions (β = -0.144, 95% CI: -0.297 to 0.010). Therefore, the effect of individual users' perceived technology protection on their actual security behavior is fully mediated through individuals' evaluation of insecurity action decisions. In other words, the change in technology protection may not influence their security behavior but does influence how they evaluate the expected outcome of insecurity action behavior, and they are more likely to adjust their security behavior accordingly.

2.5 Discussion

Due to an information system's natural interactive complexity (Perrow, 1999), information system security can be dependent on its weakest node (Anderson & Moor 2006). Indeed, the reliability of the information security systems depends on the end users as the users operating in a decentralized

environment where they share or maintain sole responsibility for their computing resources (Warkentin and Johnston 2006, 2008). The widespread assumption among security specialists is that increasing security protection will cause *a reduction* in security risks.

This study challenges this assumption by showing that the information system could be more vulnerable when security technologies cause system users to make more risky decisions. Thus, my study investigates the paradoxical relationship between security investment (i.e., adopting security technologies) and system risks (i.e., system users' risk-taking behavior) at the individual level. The findings show that system user risk-taking behaviors could significantly diminish technological protection benefits. For example, a VPN can encrypt communication between a system user's devices and targeted servers but could also motivate users to use corporate laptops more frequently in public areas (e.g., Starbucks) and use unprotected Wi-Fi. This will create a potential risk of exposure and the potential for laptops to be hacked (e.g., packets sniffing and intercepting) or stolen by those at that location.

Technological information security solutions alone may therefore not solve the information security puzzle. It is, therefore, necessary to go beyond technical considerations (Dhillon & Torkzadeh, 2006). Indeed, Angst et al. (2017) posit that the protection effectiveness of information security technologies depends on the degree of integration of the security technologies with its core operations. A technological security solution can only deliver maximum protection where the organization integrates information security technologies into its routine business processes. Surprisingly, Angst et al. (2017) found, after analyzing a large dataset of the IT security investments and data breaches of more than 5000 hospitals', that IT security investment does not lead to any reduction in data breaches no matter how well IT security is integrated but does increase the likelihood of a data breach. They furthermore concluded that a reduction in data breaches in

the healthcare sector could not be directly attributed to IT security investments, but hospitals that fail to integrate IT security systems into their core operations will suffer an even greater likelihood of a security breach.

The boundary conditions of my proposed decision model underly the theoretical foundation I applied to build this decision model, which is self-regulation theory and expected utility theory. First, the self-regulation theory assumes individuals have full autonomy when making a decision. However, such a condition may not be true in some information security contexts. Many organizations have implemented information security policies and other types of information technologies that regulate individual system users' behaviors. The information security policies may restrict individuals' decision choices when facing security threats (Bulgurcu et al., 2010; Herath & Rao, 2009), such as users always need to exercise security actions decisions regardless of the scenario. In addition, some technical controls may also limit users' decision choices. For instance, an organization may implement a strict password policy that requires users to create a complex password even when the two-factor authentication system has been adopted. Second, expected utility theory assumes individuals are fully rational. However, individuals may have bounded rationality (Simon, 1955, 2013). Thus, when applying the proposed decision model and study findings, other scholars may need to address and discuss the potential issues with the individual bounded rationality that influences individual decision choice. A possible solution to address this issue is that other scholars may add additional moderators (e.g., emotion and attitude toward information security technologies) to the decision model and provide more fruitful insights to explain the influence of information security technologies on individuals' decision choices.

2.6 Contribution to the theory

In this study, I find that security technology protection decreases security's expected utility but increases insecurity action decisions. In other words, security technologies can make the security decision less ideal decision choice and make the insecurity decision less risky and more desirable, so providing extra security protection and reducing the likelihood of breach occurrence for both decisions. On average, however, security technologies increase the likelihood of users making insecure action decisions. I find a significant mediating effect for the expected utility of insecurity action decisions but fail to find a significant mediation effect for the expected utility of security action decisions. However, it is reasonable that the expected utility of security action decisions has no significant effect. The increased utility for security action decisions could be simultaneously diminished by the decreased expected utility of insecurity action decisions, leading on average to more likely risk-taking behaviors. Van Slyke and Belanger (2020) suggest that system users deal with "*inevitable tension between information system use and information security control."* System users must balance the choices between a risky decision that maximizes the potential benefits of system use and a less risky decision that minimizes the system risks. Security technologies afford a better security environment. They may, however, trigger the system feedback loop, users re-evaluating the outcomes of the intended decisions and adjusting their security behavior accordingly. That may partially explain the paradoxical relationship between security technology investment and actual system security.

The proposed theoretical framework has the potential to explain other paradoxical behaviors by incorporating and measuring the comparable expected utility of the decisions into the same decision model. For example, information privacy literature has discovered a paradoxical relationship between individual privacy concerns and privacy behaviors. People with high privacy

concerns may disclose more personal data (Belanger & Crossler, 2011; Smith et al., 2011). The privacy concern could, under our proposed theoretical framework, be interpreted as a privacy decision was taken under the risk that individuals are concerned that their self-disclosed data might be misused. An individual's privacy decision can influence the likelihood of data misuse (i.e., more self-disclosed data leads to more risk). My decision model, therefore, would explain the paradoxical relationship that privacy concerns may increase the expected utility of non-disclosure decisions. However, such an increase may not be strong enough to mitigate the individual's expected utility of self-disclosure decisions, leading to no change in privacy behaviors. In other words, the privacy concern is necessary but not a sufficient condition for self-disclosure.

2.7 Contribution to Practice

This study makes practical contributions by explaining why and how security technology investment could lead to insecure behaviors and plausibly cause more risk exposure that puts organization information systems in danger. It is, however, worth noting that the findings should provide new, non-exhaustive, and exclusive causal explanations. It is correct to say that we have examined this paradoxical relationship at the individual level. This should not, however, diminish the contributions. Individual users are primarily a part of the information system. It is, therefore, necessary to know under what conditions our weakest node would become even more vulnerable. Willison and Warkentin (2013) suggest that system users thought processes and organizational context might significantly impact information system security control efficacy. System users who make a riskier decision due to the IT afforded security environment create opportunities for the emergence of new security threats.

I find that IT protection has no direct impact on individual security behavior. However, the effect of IT protection on security behaviors could be fully mediated through the expected utility of

security action decisions. This raises concern and calls for caution when the organization would like to adopt a more secure technology into their daily operations. I, therefore, call practitioners' attention to employees' additional risk-taking behaviors, especially when they plan to adopt or implement new information security technology.

2.8 Limitations

The first limitation comes from our experimental design. Although I randomly assigned the participants to low or high technological protection conditions in the second stage of experiment 1, it does not warrant that participants in both conditions can perceive the same magnitude change in security protection. That is because participants could presume different levels of technological security protection. However, such individual differences could be mitigated through experimental randomization (Shadish et al., 2002).

For future research, I suggest other researchers implement a two-stage experiment to address this issue further. In stage 1, the participants could be randomly assigned to either low- or high-level technological security protection scenarios. In stage 2, those participants assigned to the high-level technological protection condition would be assigned to the low-level technological protection condition, and those assigned to the low-level technological protection condition will be assigned to the high-level technological protection condition. Implementing this new design could ensure the participants in both conditions can perceive the same magnitude change in technological security protection level. In addition, when implementing the two-stage design, I call other scholars' attention to the potential learning effect.

The second limitation comes from our theory. The core idea of self-regulation theory for behavior and behavior change is that individuals execute certain actions because of the negative feedback

loop (Carver & Scheier, 1982, 1990). In order to test the hypotheses, I had to covert the self-regulation feedback loop, which is a process model, into a variance model. The researcher may implement a longitudinal study to examine the theoretical assumptions and results in a process model for future research. By doing that, we can further examine how the presence of information security technologies could cause individuals to adjust their security behavior.

The third limitation is that my experimental design does not warrant each threat scenario containing the same level of security risk, and the individual may perceive different types of security risks. Although this study used randomization to eliminate potential confounding effects from the different levels of security risks on individuals' security behaviors and to mitigate perceived different types of security risks for each participant, the possible confounding effect may still exist. To address this issue, future research can conduct a larger lab or field experiment by adding more threat scenarios to the current design or using different research methodologies to test the proposed decision model.

References:

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do it security investments matter? accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Q.*, *41*(3), 893–916. https://doi.org/10.25300/misq/2017/41.3.10

Belanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017-1041.

Bergkvist, L. (2015). Appropriate use of single-item measures is here to stay. *Marketing Letters*, *26*(3), 245-255. https://doi.org/10.1007/s11002-014-9325-y

Bergkvist, L., & Rossiter, J. R. (2007). The Predictive Validity of Multiple-Item versus Single-Item Measures of the Same Constructs. *Journal of Marketing Research*, *44*(2), 175-184. https://doi.org/10.1509/jmkr.44.2.175

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Q.*, *39*(4), 837–864. https://doi.org/10.25300/misq/2015/39.4.5

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS [Article]. *MIS Quarterly*, *34*(3), 523-A527.

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality–social, clinical, and health psychology. *Psychological Bulletin*, *92*(1), 111-135. https://doi.org/10.1037/0033-2909.92.1.111

Carver, C. S., & Scheier, M. F. (1990). Origins and functions of positive and negative affect: A control-process view. *Psychological Review*, *97*(1), 19-35. https://doi.org/10.1037/0033-295X.97.1.19

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of Formative Measurement in Information Systems Research. *MIS Quarterly*, *33*(4), 689-707. https://doi.org/10.2307/20650323

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model. *Information Systems Research*, *32*(3), 1043-1065. https://doi.org/10.1287/isre.2021.1014

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? [Article]. *Journal of Management Information Systems*, *29*(3), 157.

Chin, W. W. (1998). Commentary: Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, *22*(1), vii-xvi.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research*, *14*(2), 189-217. https://doi.org/10.1287/isre.14.2.189.16018

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Q.*, *43*(2), 525–554. https://doi.org/10.25300/misq/2019/15117

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31*(2), 285-318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach [Article]. *Information Systems Research, 20*(1), 79-98.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314. https://doi.org/10.1111/j.1365-2575.2006.00219.x

Diamantopoulos, A. (2006). The error term in formative measurement models: interpretation and modeling implications. *Journal of Modelling in Management, 1*(1), 7-17. https://doi.org/10.1108/17465660610667775

Edwards, J. R. (1992). A Cybernetic Theory of Stress, Coping, and Well-Being in Organizations. *Academy of Management Review, 17*(2), 238-274. https://doi.org/10.5465/amr.1992.4279536

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases: Opportunities And Challenges. *Academy of Management Journal, 50*(1), 25-32. https://doi.org/10.5465/amj.2007.24160888

Finch, J. (1987). THE VIGNETTE TECHNIQUE IN SURVEY RESEARCH [Article]. *Sociology, 21*(1), 105-114.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320-326. https://doi.org/https://doi.org/10.1016/j.im.2012.08.001

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236.

Hair, J. F., Jr. (2006). *Multivariate data analysis* (6th ed. ed.). Pearson Prentice Hall.

Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis : a regression-based approach* (Second edition. ed.). The Guilford Press.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Q., 34*(3), 549–566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats To The Human Asset Through Sanctioning Rhetoric [Article]. *MIS Quarterly, 39*(1), 113-A117.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica, 47*(2), 263-291. https://doi.org/10.2307/1914185

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly, 38*(2), 451-A453. https://doi.org/10.2307/26634934

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory Standards and Organizational Information Security. *Information Systems Research, 27*(1), 70-86. https://doi.org/10.1287/isre.2015.0607

Lee, J. S., Keil, M., & Shalev, E. (2019). Seeing the Trees or the Forest? The Effect of IT Project Managers' Mental Construal on IT Project Risk Management Activities. *Information Systems Research*, *30*(3), 1051-1072. https://doi.org/10.1287/isre.2019.0853

Liang, H., & Xue, Y. (2009). Avoidance Of Information Technology Threats: A Theoretical Perspective [Article]. *MIS Quarterly*, *33*(1), 71-90. https://doi.org/10.2307/20650279

Liang, H., Xue, Y., Alain, P., & Wu, Y. A. (2019). What Users Do Besides Problem-Focused Coping When Facing It Security Threats: An Emotion-Focused Coping Perspective [Article]. *MIS Quarterly*, *43*(2), 373-394. https://doi.org/10.25300/MISQ/2019/14360

Lohmoller, J. B. (1988). The PLS Program System: Latent Variables Path Analysis with Partial Least Squares Estimation. *Multivariate Behav Res*, *23*(1), 125-127. https://doi.org/10.1207/s15327906mbr2301_7

Lowry, P. B., & Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. *IEEE Transactions on Professional Communication*, *57*(2), 123-146. https://doi.org/10.1109/TPC.2014.2312452

Maruping, L. M., & Magni, M. (2015). Motivating employees to explore collaboration technology in team contexts. *MIS Q.*, *39*(1), 1–16. https://doi.org/10.25300/misq/2015/39.1.01

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory [https://doi.org/10.1111/j.1559-1816.2000.tb02308.x]. *Journal of Applied Social Psychology*, *30*(1), 106-143. https://doi.org/https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward A Unified Model Of Information Security Policy Compliance [Article]. *MIS Quarterly*, *42*(1), 285.

NIST. (2012). *Security and privacy controls for federal information systems and organizations* (Rev. 4, initial public draft. ed.). U.S. Dept. of Commerce, National Institute of Standards and Technology.

Nozick, R. (1969). Newcomb's Problem and Two Principles of Choice. In N. Rescher (Ed.), *Essays in Honor of Carl G. Hempel: A Tribute on the Occasion of his Sixty-Fifth Birthday* (pp. 114-146). Springer Netherlands. https://doi.org/10.1007/978-94-017-1466-2_7

Petter, S., Straub, D., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. *MIS Quarterly*, *31*(4), 623-656. https://doi.org/10.2307/25148814

PWC. (2014). *The Global State of Information Security Survey 2015*.

PWC. (2015). *The Global State of Information Security Survey 2016*.

Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm Performance Impacts of Digitally Enabled Supply Chain Integration Capabilities. *MIS Quarterly*, *30*(2), 225-246. https://doi.org/10.2307/25148729

Rosenblueth, A., Wiener, N., & Bigelow, J. (1943). Behavior, Purpose and Teleology. *Philosophy of Science*, *10*(1), 18-24.

Savage, L. J. (1954). *The foundations of statistics*. Wiley.

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, *32*(2), 314-341. https://doi.org/10.1080/07421222.2015.1063315

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Wadsworth Cengage Learning.

Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, *69*(1), 99-118.

Simon, H. A. (2013). *Administrative behavior*. Simon and Schuster.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights Into The Problem Of Employee Information Systems Security Policy Violations [Article]. *MIS Quarterly*, *34*(3), 487.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989-1015. https://doi.org/10.2307/41409970

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making [Article]. *MIS Quarterly*, *22*(4), 441-469.

Tirenin, W., & Faatz, D. (1999, 31 Oct.-3 Nov. 1999). A concept for strategic cyber defense. MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat. No.99CH36341),

Van Slyke, C., & Belanger, F. (2020). Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective. *Computers & Security*, *99*, 102064. https://doi.org/https://doi.org/10.1016/j.cose.2020.102064

Vance, A., Brinton Anderson, B., Brock Kirwan, C., & Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG) [Article]. *Journal of the Association for Information Systems*, *15*(10), 679-722.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory [Article]. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Von Neumann, J., & Morgenstern, O. (1947). *Theory of games and economic behavior* (Second edition. ed.). Princeton University Press.

Wiener, N. (1948). *Cybernetics; or, Control and communication in the animal and the machine*. J. Wiley.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View Of Employee Computer Abuse [Article]. *MIS Quarterly*, *37*(1), 1.

Wolff, J. (2016, 5-8 Jan. 2016). Perverse Effects in Defense of Computer Systems: When More is Less. 2016 49th Hawaii International Conference on System Sciences (HICSS),

Wood, R. E., Goodman, J. S., Beckmann, N., & Cook, A. (2008). Mediation testing in management research: A review and proposals. *Organizational Research Methods*, *11*(2), 270-295. https://doi.org/10.1177/1094428106297811

Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. the 26th International Conference on Information Systems, Las Vegas, NV.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330-340. https://doi.org/10.1108/09685220910993980

Appendix A Descriptive Statistics and Correlation Coefficients

Table 10. Descriptive Statistics and Correlation Coefficients

	Mean	Std	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1 Breach_U1	5.14	1.75	1.00																	
2 Breach_U2	5.26	1.78	.907**	1.00																
3 Breach_U3	5.05	1.87	.843**	.881**	1.00															
4 Breach_U4	5.05	1.88	.833**	.869**	.895**	1.00														
5 Breach_U5	5.16	1.79	.838**	.868**	.869**	.863**	1.00													
6 Act_N_T1	4.93	1.54	-.290**	-.304**	-.343**	-.324**	-.294**	1.00												
7 Act_N_T2	4.73	1.59	-.360**	-.366**	-.406**	-.391**	-.370**	.831**	1.00											
8 Act_N_T3	4.62	1.58	-.327**	-.352**	-.359**	-.360**	-.322**	.772**	.871**	1.00										
9 Funct_U1	3.85	1.96	-.354**	-.377**	-.413**	-.403**	-.390**	.369**	.404**	.372**	1.00									
10 Funct_U2	3.66	1.91	-.353**	-.363**	-.395**	-.398**	-.371**	.373**	.420**	.396**	.901**	1.00								
11 Funct_U3	3.95	1.86	-.300**	-.299**	-.333**	-.337**	-.308**	.293**	.340**	.312**	.753**	.759**	1.00							
12 Funct_U4	3.81	1.84	-.304**	-.287**	-.329**	-.333**	-.298**	.331**	.365**	.346**	.817**	.816**	.798**	1.00						
13 N_Act_T1	5.54	1.21	.347**	.310**	.356**	.356**	.320**	-.258**	-.283**	-.291**	-.371**	-.372**	-.291**	-.300**	1.00					
14 N_Act_T2	5.50	1.25	.330**	.297**	.356**	.344**	.301**	-.257**	-.267**	-.274**	-.382**	-.377**	-.296**	-.315**	.889**	1.00				
15 N_Act_T3	5.44	1.23	.321**	.299**	.370**	.375**	.321**	-.260**	-.276**	-.258**	-.378**	-.378**	-.308**	-.304**	.862**	.877**	1.00			
16 Protec	1.53	0.50	-.536**	-.538**	-.601**	-.615**	-.547**	.446**	.514**	.470**	.720**	.716**	.617**	.632**	-.432**	-.431**	-.431**	1.00		
17 Realistic	5.54	1.04	0.08	0.08	0.06	0.07	0.03	0.01	0.06	0.03	-0.01	-0.01	0.04	0.01	0.06	0.07	.123**	0.00	1.00	
18 Decision	1.60	0.49	.200**	.182**	.198**	.201**	.192**	-.157**	-.176**	-.159**	-.253**	-.210**	-.178**	-.227**	.250**	.216**	.240**	-.296**	0.08	1.00

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Chapter 2 Postscript

This study explored the tension between individual rational decisions and information security technologies. When individuals face security threats requiring them to make an immediate security decision, they make decisions under uncertainties. When the system environment is uncertain (i.e., caused by the change of security technology protection), on the one hand, the individual may exercise security action decisions to reduce security risks further. However, by doing this, they must comprise the system's functionality and reduce their work productivity. On the other hand, the individuals may exercise insecurity action decisions to retain the system functionality and work productivity. However, by doing this, they are facing the potential negative consequences caused by a security breach. The study shows that individual cognitive evaluation of two mutually exclusive decision outcomes is responsible for their chosen actions.

Individual decision point, in chapter 2, is whether or not the individual system users should relax their security behaviors (i.e., choose less secure but more convenient decisions when the information security technology is present). The information security system will become less reliable if the individual users make more risky decisions, introducing security system weaknesses and failure points. Thus, the technology-induced system failure points could diminish additional security technology protection benefits, causing the information system to become less sustainable.

Chapter 3 Preface

Two-factor authentication uses any combination of an authentication modality or the combination of multiple features of different authentication modalities, and it has been argued for many years that it can protect against the pitfalls of the password and PIN-only authentication system. While we hope to add additional authentication factors to protect information systems better, this study demonstrates the potential embedded risks in the added second authentication factor.

This study investigates the potential downside of two-factor authentication based on the perspective of researchers. When designing a new security technology artifact, we are facing the dilemma that we need to design a more reliable and strict security system that may sacrifice system useability. However, the user often puts system useability before information security, causing an increase in overall system vulnerabilities. This study demonstrates the reliability of information security systems could rely not only on their weakest node but also on the joint efforts of all users and system developers (i.e., security researchers).

This study responds to my thesis theme by demonstrating the induced security risks embedded in the second authentication factor, causing a potential decrease in the two-factor authentication system's reliability, especially when the system developer has purposely used a weaker form of security protection to retain a sufficient level of system useability in term of users' convenience and cost of implementation.

Chapter 3. The Case for Two-Factor Authentication- Evidence from a Literature Review*

3.1 Introduction

Security is critical for an information system (IS). When adopting information security technologies properly, information security technologies can help increase firms' value (Bose & Alvin Chung Man, 2019). However, the organization and the users always face the dilemma of balancing information security and information system usability(Dhillon et al., 2016; Lampson, 2009; Lennartsson et al., 2021). On the information security development side, when designing a new security system, the researcher sometimes has to sacrifice system useability to achieve a sufficient level of security (Cranor & Buchler, 2014). On the users' adoption and use side, the user often puts system useability before security, causing an increase in overall system threats (Fagan & Khan, 2016). The information security threats include natural and human-made disasters, errors by employees, viruses, hackers, etc. (Karen D. Loch et al., 1992). Organizations tend to rely on technology solutions or employees' compliance with information security policies to reduce information security threats. However, the literature has shown that the increases in information security technologies have little or no effect on reducing the number of security breaches (Angst et al., 2017).

Nevertheless, we assume that it is more effective to implement a more sophisticated and comprehensive authentication scheme to compensate for man-made disasters, human errors, and hacker threats (Cheong et al., 2014; Connie et al., 2004; Kumari & Khan, 2014; Yang et al., 2008). An example of such increased complexity is replacing a single-factor authentication-based system with a multi-factor authentication-based system. In general, authentication is an information security method that intends to protect against any illegitimate access to an individual device or

* A previous version of this paper was published as Wang, P., & Baskerville, R. (2019). The Case for Two-Factor Authentication- Evidence from a Systematic Literature Review. Paper presented at the Twenty-Third Pacific Asia Conference on Information Systems, Xi'an, China.

data server (Dasgupta et al., 2016). The most widely adopted authentication method is the password or personal identification number (PIN) based on single-factor authentication. Despite this wide adoption, many researchers find weaknesses in this method (Cheong et al., 2014; Connie et al., 2004; Kumari & Khan, 2014; Yang et al., 2008), including but not limited to the password or PIN being lost, forgotten, illicitly acquired by direct observation, hacked by dictionary attacks, or attacked by online guessing.

Consequently, using a combination of multiple factors has become a prevalent trend on the assumption that it provides more secure, more resilient, and more robust access to digital systems. It is widely assumed that security for a password-protected system will be improved by expanding the access control to include two-factor authentication. Intuitively, adding an additional factor(s) to the existing single-factor authentication system is an obvious solution. However, our research suggests that this assumption is both unproven and questionable. In contrast, our study finds that the evidence in the literature points to many security weaknesses in various two-factor authentication schemes. Also, adding additional authentication factors can cause operability difficulties such as high computing power requirements, low reliability, and high operating cost. Therefore, our research question is:

How do additional authentication factors affect security risk in relation to security costs?

A superficial review of the literature suggests that a dearth of research may support the assumed efficacy of two-factor authentication. Accordingly, we undertook a systematic literature review on this topic. Our objectives are to evaluate, synthesize and present the empirical findings on two-factor authentication to date and provide an overview of the topics that have been studied. We will use these findings and implications to suggest future research directions.

This study finds an evident growth in interest in two-factor authentication. More than half of the relevant research articles were published after 2013. There is strong empirical evidence showing how two-factor authentication can deliver superior performance for information security. In fact, the available evidence indicates the opposite: that adopting two-factor authentication brings a lot of unexpected risks.

3.2 Authentication Challenges

Authentication is an information security method to protect against any illegitimate access to digital devices and data servers (Dasgupta et al., 2016). As a baseline, we will briefly review research on the security effects of improving one-factor authentication. Passwords are a prevalent and traditional form of one-factor authentication.

The problem of poor password selection and hygiene is well-known. Strong passwords are long, random, contain multiple character types, and are unique. Strong passwords introduce entropy into the intrusion process. It takes more work to attack such passwords. But we know that people will choose simple, easily cracked passwords without improving the password-setting process. For example, Hunt 2011[1] analyzed 37,608 passwords revealed as part of a Sony breach. He found that half of these passwords were less than eight characters in length, and only about one percent used alphanumeric characters.

Two-factor authentication uses any combination of an authentication modality or any combination of multiple features of different authentication modalities. In general, two-factor authentication uses a combination of features taken from:

- *The Knowledge Factor is what we know, such as a password*
- *The Possession Factor is what we have, such as a smart card*
- *The Inherent Factor is what we are, such as a fingerprint*

[1]https://www.troyhunt.com/brief-sony-password-analysis/

Many researchers claim that two-factor authentication can ensure against the pitfalls of single-factor authentication, for example, the Man-in-the-Middle attack and Phishing (e.g., Kiljan et al., 2016; Sarel & Marmorstein, 2006; Yoo et al., 2015). They believe that using a combination of multiple features is an ongoing trend to provide secure, resilient, and robust access to preserve the legitimacy of digital users. That is, the use of two-factor authentication for information security is an improvement.

Others are less confident. For example, the most common two-factor online banking authentication scheme combines the traditional password process with an SMS challenge code sent to the user's mobile phone. The user must possess this challenge code to complete the login process. Schneier (2005) explains how such a simple two-factor (or two-channel) approach does little to prevent Man in the Middle attacks. Such approaches can still be easily defeated by lax security practices, such as storing plaintext passwords on an unencrypted mobile phone. If the phone is stolen, the attacker controls both factors, and the users even suffer a higher risk due to the fact that the bank usually allows higher transaction amounts with two-factor authentication.

We question whether introducing a second factor in the authentication process (such as a token) is more effective than hardening one factor (such as improving password practices). With this background in mind, we set about a systematic literature review to determine what we know about the efficacy of two-factor authentication.

3.3 Systematic Literature Reviews Methodology

The notion of a systematic literature review first arose in the evidence-based practices of medicine. A systematic literature review synthesizes "… research in a systematic, transparent and reproducible manner to inform policy and decision-making about the organization. … Systematic

reviews differ from traditional narrative reviews by adopting a replicable, scientific and transparent process, in other words, a detailed technology, that aims to minimize bias through exhaustive literature searches of published and unpublished studies and by providing an audit trail of the reviewers' decisions, procedures, and conclusions." (Tranfield et al., 2003, p. 209)

In this study, we are interested in the efficacy of two-factor authentication and the evidence of this efficacy in the research literature. Two-factor authentication has been extensively studied in computer science and information system fields, and many studies have addressed the same security challenges by using *different* two-factor authentication approaches. Many other studies have tried to manage the security challenges using the same two-factor authentication approaches but using an improved or modified algorithm. These similar but comparable studies provide a perfect environment to apply a systematic literature review for comparing, interpreting, and translating the key concepts in the selected articles.

3.3.1 Data Collection Process

Two databases were selected: the ABI/Inform Collection and EBSCOhost Database, and our search query is: (1) "two factor authentication"; (2) "two-factor authentication"; (3). 2FA; (4) "dual factor authentication";(5)"dual-factor authentication"; (6) "two-stage authentication"; (7) "two stage authentication"; (8) "two-step authentication"; (9) "two step authentication"; (10) "two-factor verification"; (11) "two-factor verification"; (12) "multi-factor authentication"; (13) "multi factor authentication"; (14) "multiple factor authentication"

This review applied different criteria in the different search and analysis stages. First, the time frame for this systematic review is from 2000 to 2021. The study must be written in English and published in a peer-reviewed academic journal. Second, studies were eligible for inclusion in this review only if they focused on two-factor authentication. Third, as our research questions are

concerned with two-factor authentication, articles will be excluded if the research focus is on single or multiple authentications (more than two factors). The selected articles must focus on the development of any combination of two-factor authentication. Finally, given that our focus is on a search for empirical–evidence that evaluates the effectiveness of two-factor authentication in general, papers without a rigorous research design (e.g., an editorial note or an industry survey) and papers based merely on expert opinions were excluded. Excluded also from the search were books, conferences, news, editorials, workshop sessions, discussion, comments, etc. In this initial search, over one thousand articles were identified in ABI/Inform and EBSCOhost. All results were exported separately to an Endnote database for further analysis.

Based on an analysis of the title, keywords, and abstract, we eliminated all irrelevant articles, leaving 55 articles that were brought forward for a detailed analysis (see Table 1). We performed a detailed analysis of all 55 articles and classified the selected articles into different groups. Since our study focuses on synthesizing and evaluating any new or improved two-factor authentication scheme, we excluded papers that lacked an appropriate, rigorous, empirical research design. This exclusion left 55 articles.

We used the Nvivo to analyze and synthesize the 55 selected articles creating a table in Microsoft Word for each Article. These tables supported a comparison of the articles' research questions/objectives and proposed solution(s). The detailed findings are discussed in the finding section.

Table 3- 1. Studies Selected for Analysis

Year	First Factor	Second Factor	Context	Reference
2004	Token	Fingerprint	General Information Systems	Jin et al. (2004)
2004	Password	Palmprint	General Information Systems	Connie et al. (2004)
2007	Password	Smartcard	Telecare Medical Information Systems	Huang and Hou (2007)

2007	Biometric keys	Biometric Factor	Telecare Medical Information Systems	Bhargav-Spantzel et al. (2006)
2007	Token	Face	General Information Systems	Pang et al. (2007)
2008	Password	Fingerprint	General Information Systems	Khan et al. (2008)
2008	Password	Smartcard	General Information Systems	Yang et al. (2008)
2011	Password	RFID	Wireless Local Area Network	Guo et al. (2011)
2011	Password	Token	Mobile & Cloud Systems	Cheng (2011)
2013	Watermark	RFID	Retail Information Systems	Ting and Tsang (2013)
2013	Password	Smartcard	Telecare Medical Information Systems	Cao and Zhai (2013)
2013	Password	Token	General Information Systems	Lat et al. (2013)
2013	Password	Token	Financial Information Systems	Yunlim Ku et al. (2013)
2014	Password	Smartcard	Wireless Sensor Network	Hsieh and Leu (2014)
2014	Password	Fingerprint	General Information Systems	Go et al. (2014)
2014	Password	Smartcard	General Information Systems	Wei et al. (2014)
2014	Password	Smartcard	General Information Systems	Kumari and Khan (2014)
2014	Password	Smartcard	Telecare Medical Information Systems	Islam and Khan (2014)
2014	Password	Smartcard	Mobile Information Systems	Xie et al. (2014)
2014	Password	NFC	Mobile Information Systems	Cheong et al. (2014)
2014	Faceprint	Fingerprint	General Information Systems	Ma et al. (2014)
2014	Password	Smartcard	Wireless Sensor Network	Kim et al. (2014)
2014	Password	Smartcard	General Information Systems	Juan and Xiao-Ling (2014)
2015	Password	Smartcard	Telecare Medical Information Systems	Chaudhry et al. (2015)
2015	Password	Smartcard	General Information Systems	Jiang et al. (2015)
2015	Password	Smartcard	Wireless Sensor Network	Chang et al. (2015)
2015	Password	Gait	General Information Systems	Hoang et al. (2015)
2015	Password	Gait	General Information Systems	Ntantogian et al. (2015)
2015	Password	Smartcard	Telecare Medical Information Systems	Arshad et al. (2015)
2015	Password	Smartcard	General Information Systems	Wang et al. (2015)
2015	Password	Signature	General Information Systems	Khan et al. (2015)
2015	Password	Smartcard	General Information Systems	Arshad and Nikooghadam (2015)
2016	Password	Decentralized certificate authority	Automobile Information Systems	Wang et al. (2016)
2016	Password	Smartcard	Wireless Sensor Network	Jiang et al. (2016)
2016	Password	Smartcard	General Information Systems	Xie et al. (2016)
2016	Password	Smartcard	General Information Systems	Gupta and Dhar (2016)
2016	Password	Token	Financial Information Systems	Mann and Loebenberger (2017)
2017	-	-	Education	Albayram et al. (2017)
2018	Password	Smartcard	General Information Systems	Ravanbakhsh et al. (2019)
2018	Password	Tap	Mobile Information Systems	Nguyen and Memon (2018)
2018	Password	Smartcard	General Information Systems	Malina et al. (2018)

2018	-	-	Literature Review	Pomputius (2018)
2019	Location	Device Characteristics	Internet of Things	Aman et al. (2019)
2019	Token	NFC	General Information Systems	Pranata and Hargyo Tri (2019)
2020	Voiceprint	Password or Fingerprint	Voice of Internet Systems	Elshamy et al. (2021)
2020	Password	Token	General Information Systems	Jover (2020)
2020	-	-	Literature Review	C. Wang et al. (2020)
2020	-	-	Literature Review	Guma et al. (2020)
2020	Password	Token	Financial Information Systems	Yin et al. (2020)
2020	Password	Smartcard	Telecare Medical Information Systems	Sherali and Falah (2020)
2020	Password	QR Code	General	Naser et al. (2020)
2021	Password	Keystroke	General Information Systems	Čapek and Hub (2021)
2021	-	-	Financial Information Systems (Survey)	Kassim, Ramayah, et al. (2021)
2021	Password	Smartcard	Financial Information Systems	Tsai and Su (2021)
2021	Password	Smartcard	Telecare Medical Information Systems	Gupta et al. (2021)

3.4 Findings

In this section, we discuss the overall evaluation and the detailed evaluation results that regard the strength of the evidence of selected articles.

Based on these 55 relevant articles, we can see a trend of rising attention to two-factor authentication. 32 (58%) of the selected articles were published after 2015. Among the 55 articles, 13 (24%) are mainly based on adding biometric factors such as fingerprints and palm prints to a password-only authentication scheme. The 35 articles (64%) focus on improving system security by adding a possession factor (such as a smartcard or token). Among 55 selected articles, the smartcard and password are the most studied two-factor authentication scheme, followed by fingerprint, digital key, gait recognition, face recognition, radio frequency identification, one-time password, gait, and palm print.

Guma et al. (2020) provide a good summary for classifying threat models in the two-factor authentication schema. The identified threat models include attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity, and attacks against system availability. We had expected to find evidence in the literature that would guide us in deciding which of the available authentication factors worked reliably together in which situations. It was somewhat surprising that nearly all related studies dealt with weaknesses in the various known factors. The research pattern of the two-factor authentication discipline has fallen into an undesirable "break-fix-break-fix" cycle, and a lot of effort has been devoted, but little progress has been made (D. Wang et al., 2020).

In general, some studies examined these weaknesses, and we designated the knowledge from these studies as *problem-centered weaknesses*. Many of these studies examined such weaknesses and proposed solutions, and we designated the knowledge from these studies as *solution-centered weaknesses*. Also, many of these studies examine the weakness and strengths of other studies with the focus on improving users' useability when implementing the news security schema. We designed the knowledge from these studies as a *user-centered weakness.* In the selected studies, problem-centered weaknesses arose from studies of compromises of the available factors. Solution-centered weaknesses arose from the development of improvements related to the available factors. User-centered weakness arose from the balance between system security and system useability.

3.4.1 Theme 1. Problem-centered Weaknesses in Authentication Factors

Password Weaknesses: Password or PIN authentication is widely used on its own in single-factor settings. Not surprisingly, it is also commonly used as one of the two factors in two-factor authentication. Given its prominence, password compromises are well studied. Many studies

indicate that passwords or PINs can be lost, forgotten, illicitly acquired by direct observation, and hacked by dictionary attacks or online guessing attacks (Cheong et al., 2014; Connie et al., 2004; Kumari & Khan, 2014; Yang et al., 2008). Such attacks are made easier when users are permitted to choose weak passwords. Password-based authentication usually requires the servers to maintain a verifier table to match the inserted password with the stored password before granting access (Kumari & Khan, 2014). If the verifier table is exposed, it can be compromised by various automated methods, even while still encrypted. In addition, many users practice poor security hygiene by using the same PINs or passwords for many, if not all, of their accounts. Compromise of one of their accounts can lead to compromise of their other accounts (Wang et al., 2015).

Two-factor authentication is supposed to provide more secure and robust ways to protect sensitive information than passwords alone. Password-based authentication has well-known weaknesses. However, our systematic literature review reveals findings suggesting that the other possible factors in two-factor authentication also suffer many risks. These will be discussed below.

Weaknesses in biometric-based two-factor authentication

Template compromises: Adding biometric factors into the authentication scheme has inherent advantages, such as increasing customer trust(Kassim, Ramayah, et al., 2021). A biometric-based two-factor authentication system does not require the users to carry a physical key or memorize a password (Cheong et al., 2014). However, these inherent characteristics also bring challenges. Ntantogian et al. (2015) admit that biometric-based two-factor authentication systems require very high protection for the extracted template. Due to impersonation attacks, users' immutable biometric templates will be useless if the templates are stolen. The biometric templates from users are unchangeable, and the new templates cannot be assigned when compromised (Pang et al., 2007). Many researchers indicate that it is critical to create a *concealed* biometric-based two-factor

authentication (Ma et al., 2014; Pang et al., 2007). The sensitive nature of biometric data has alarmed the public's concern about privacy issues (Connie et al., 2004). Khan et al. (2011) find that if users' biometric data leaks to an unauthorized party, the data could be misused. For example, unauthorized users may use the stolen data to log into users' accounts in multiple accounts where the same biometric templates exist. It can result in lost integrity for the whole security system. The only remedy is to replace the stolen data with other biometric templates. However, users only have a limited number of biometrics traits. Also, Ma et al. (2014) find that biometric data cannot be kept in explicit form; it must be converted into encrypted form. If the biometric template needs to be stored on a portable device, such as a mobile phone or laptop, it suffers a higher risk of theft and malware. The users become more vulnerable to security and privacy threats, not less. Thus, while biometric-based two-factor authentication aims to protect individual private data, many people show their privacy concern when using such techniques for two-factor authentication (Pomputius, 2018).

Costliness: Compared with other authentication systems, a biometric-based authentication system is expensive because a biometric-based two-factor authentication system typically increases deployment cost and incurs the complexity of integrating existing security systems with biometric technologies(Tsai & Su, 2021). The high implementation cost is another concern for the companies who want to adopt a biometric-based two-factor authentication system. Using multiple biometric measurement and storage devices will impose high additional costs. For example, designing a new and more sophisticated user interface affects usability, generating additional management complexity (Cheong et al., 2014; Connie et al., 2004; Lat et al., 2013).

Reliability: Biometrics factors seem reasonably secure and reliable because individuals' physical characteristics are literally part of who they are (Pomputius, 2018). However, biometric

authentication suffers from high false acceptance and rejection rates (Kassim, Ramayah, et al., 2021; Pang et al., 2007). The biometric features of the same subject cannot be extracted exactly the same, and the system has to tolerate a certain level of data noise. As a result, the authentication system may fail before the user can get access (Ntantogian et al., 2015). Natantogian et al. (2015) further indicate that the encrypted biometric template can increase even more intra-variance, resulting in even higher false rejection rates and false acceptance rates. Therefore, system owners must determine their optimal balance between security and performance.

Weaknesses in Possession Factor Authentication

Smartcard compromise: In two-factor authentication literature, smart-card-based two-factor authentication is the most highly studied. This authentication method requires the user to carry a physical chip-enabled device, and it requires the user to insert it into a reading device before accessing his/her account. The smart card can provide extra security layers, but its stored secret information can be revealed with techniques such as power analysis, reverse engineering, fault injection attacks, and other kinds of side-channel attacks (Islam & Khan, 2014; Wang et al., 2015). Compared with biometric-based authentication, the inherent disadvantage of smart card-based authentication is that the system is very vulnerable to impersonation attacks. It is hard for the system to distinguish the legitimate or malicious access because both the smart card and the password can be stolen (Chaudhry et al., 2015). Chaudhry et al. (2015) conclude that the smart-card-based two-factor authentication is unsuitable for practical deployment if the server cannot distinguish legitimate from malicious users' access.

Impersonation: Impersonation attacks are highly related to the lost/stolen smart card. If the smart card is lost or stolen, there is no effective way to prohibit it from being misused (Kumari & Khan, 2014). The confidential information stored in the smart card can be extracted by an external device

that physically monitors its power consumption. There are also other kinds of side-channel attacks if the end users' authentication request cannot be transmitted via a secure channel during the login and key agreement protocol (He et al., 2013; Wei et al., 2014). A smart card is also vulnerable to password guessing attacks, especially when it is stolen. Chaudhry et al. (2015) find that an adversary can get the password with the help of certain offline methods unless the server is able to distinguish a valid smart card from a lost one. They argue that the authentication system should provide a proper revocation method to handle a lost smart card. In addition, the compromise of information stored in the smart card can also reveal users' identities. Many studies indicate that the user's privacy protection is an important requirement when implementing a smart card-based authentication system (Chang et al., 2015; Dasgupta et al., 2016; Gupta & Dhar, 2016; Jiang et al., 2016; Kumari & Khan, 2014). Issuing a new or replacement smart card can dramatically increase system cost, and additional equipment is also needed to read and store data into the smart card (Gupta & Dhar, 2016).

Token weaknesses: Token-based two-factor authentication is another popular method in this category. The token can be a hardware, software, mobile phone, or cloud-based QR code (Cheng, 2011). Cheng (2011) found that such tokens suffer several drawbacks, such as poor token interoperability, poor inter-system compliance, high hardware and support cost, and poor portability. Token-based security suffers risks similar to smart cards if the token is stolen or lost. It is not very convenient for the end users because it requires the user to have specialized hardware that may need to be replaced if it has an unreplaceable battery or restrictions on the number of uses (Lat et al., 2013). Besides that, Ku et al. (2013) find that some one-time use tokens only use a 64-bits password. It makes the authentication system vulnerable to offline password guessing attacks (He et al., 2013; Yunlim Ku et al., 2013; Y. Ku et al., 2013).

3.4.2 Theme 2. Solution-Centered Weaknesses in Authentication Factors

According to the previously synthesized findings, we find that two-factor authentication can be problematic when both factors have security issues. Not surprisingly, much of the research in the selected articles involves first highlighting one of the serious problems with two-factor authentication and second proposing a new method for two-factor authentication that improves the existing approaches. In the following section, we discuss the issues that are indirectly evidenced by the proposed security solutions offered in the selected articles.

Biometric-based two-factor authentication

Compared with other kinds of two-factor authentication, biometric-based two-factor authentication does not require the user to carry a physical key or memorize additional knowledge (Cheong et al., 2014). However, many selected articles indicate how biometric-based two-factor authentication has three major issues: a severe privacy protection requirement, high implementation and operation costs, and both high false rejection rates and high false acceptance rates (Pomputius, 2018).

Lack of Biometric Cryptosystems: With respect to the severe privacy protection requirement, Hoang et al. (2015) proposed using a biometric cryptosystem to maintain the security and privacy of the biometric system. Their approach allows the user to store this sensitive data on their mobile devices instead of the system server. They propose a gait-based two-factor authentication system that verifies users' legitimacy. The system consists of a stored cryptographic key that is biometrically encrypted by gait templates collected from a mobile accelerometer. This pre-collected gait template will be used only once and discarded after completing the authentication process. The Hoang et al. (2015) solution aims to solve the biometric privacy issue and protect users' sensitive data from any server compromise. Because the system collects the gait template

without any user interactions, it is highly convenient. However, Hoang et al. (2015) admit that gait is less discriminating and noisier than other biometric modalities such as scanning the iris, fingerprint, face, etc. They report an average false rejection rate of over 15%, quite high compared with other methods, such as a smartcard or token-based two-factor authentication. In addition, the pre-collected gait template can only be used once. Because the system requires enough time to collect a new gait template after one-time use, the system will not support frequent access authentication during short periods

Lack of Hash Functions: Another stream of the literature proposes using hash functions to encrypt the extracted biometric templates (Connie et al., 2004; Khan et al., 2011; Ntantogian et al., 2015; Pang et al., 2007). Ntantogian et al. (2015) proposed a Biohash technique to protect users' data. The Biohash technique can transform a biometric template into a noninvertible bit stream using the Biohash algorithm and a user token. Ntantogian et al. (2015) claim that this token and biometric-based two-factor authentication scheme is more secure because the individual user must provide a unique token for authentication and require authentication by a biometric feature. In addition, Pang et al. (2007)also propose tokenized biometric data as a measure to prevent server comprises. If the stored token-based biometric data is compromised, the system will issue a new tokenized biometric template.

Users Have Only a Limited Number of Biometric Traits: Because all biometric templates are tokenized, the system can convert the same biometric trait, such as the same fingerprint, into different bit streams through a hash function (Connie et al., 2004). Further, users can combine the same biometric trait with different tokens for use with multiple accounts. In this way, it reduces the systematic risk that might otherwise occur if a user's biometric data are stolen. By combining the token and the biometric template through a hash function, we can remedy the weakness of a

biometric-based authentication system that depends on the users' limited number of biometrics traits.

High Implementation and Operating Costs: With respect to cost reduction, Hoang et al. (2015) is the only study concerned about cost reduction. Hoang et al. (2015) claim gait-based two-factor authentication takes advantage of a fuzzy commitment scheme, so their two-factor authentication only requires small storage space and low computational complexity. However, as we indicated in the previous section, computing power and storage space are only part of the full system. Multiple biometric measurement devices, such as fingerprint readers and face traits scanners, could cost a lot. Therefore, we argue that Hoang et al. (2015)'s cannot change the fact that biometric-based two-factor authentication could be the most expensive system compared with other kinds of two-factor authentication systems.

High False Rejection and Acceptance Rates: With respect to reducing false rejection and acceptance rates, no study in our selected articles offered a means to effectively reduce the false rejection rate and false acceptance rate with one exception. A potential solution to decrease such a high false-rejection rate is to incorporate biometric factors with knowledge factors. Nguyen and Memon (2018) develop a tap and password-based two-factor authentication protocol. The protocol allows users to tap a memorable melody (i.e., tap-password) of their choice by using the smartwatch. The program will store the users' psychological and behavioral characteristics of tap-password. After running several experiments, Nguyen and Memon (2018) show that tap-password-based two-factor authentication could achieve an accuracy of 98.7% with a false positive rate of only 0.98%. However, no evidence shows that a biometric-based two-factor authentication system can achieve the same accuracy as other kinds of two-factor authentication systems, such as

smartcard-based two-factor authentication that could deliver close to 0% false authentication indications.

Possession-Based Two-Factor Authentication

Possession-based two-factor authentication, especially smartcard based, are most studied. A possession-based authentication system requires the user to carry a physical key or token to access the system. The physical keys or token could be a smart card or mobile device that can generate or receive one-time access codes. Many selected articles indicate that a possession-based two-factor authentication system can be very vulnerable when the smart card or one-time password token is stolen. Protecting the information stored in the smart card or mobile device is a major challenge.

Lack of Smart Card Encryption: The information stored in the smart card cannot be in plaintext. Kim et al. (2014) indicate that hackers could use all the information stored in the smart card to attack users' accounts, so encrypting the information stored in the smartcard and realizing user anonymity is critical. Several techniques were proposed in the selected articles. Juan et al. (2014) claimed that an elliptic curve cryptosystem could help smartcard-based two-factor authentication resist impersonation attacks, internal attacks, internal offline guessing attacks, server spoofing attacks, etc. However, the author did not explain clearly how the elliptic curve cryptosystem works and how they use it in their proposed authentication system. Jiang et al. (2016) also used elliptic curve cryptography to design an untraceable two-factor authentication system. They claim their proposed authentication method could compensate for the missing security features necessary for real-life performance. However, Jiang et al. (2016) only performed a security analysis to evaluate their authentication method and did not use any empirical data. Their findings and arguments may not hold in a real-world situation. Chaudhry et al. (2015) and Arshad et al. (2015) also use the

elliptic curve cryptography technique to achieve user anonymity. However, these studies also neglect the use of a simulation or experiment to support their findings. The evidence to support their arguments is weak.

Lack of User Anonymity: Another stream of literature uses dynamic ID-based techniques to achieve user anonymity and un-traceability (Cao & Zhai, 2013; Chang et al., 2015; Islam & Khan, 2014; Wang et al., 2015). Wang et al. (2015) claimed that the dynamic ID-based technique is simpler and more robust. Dynamic ID techniques can help the authentication system achieve security and privacy simultaneously by using public-key encryption with proper padding mechanisms. Chang et al. (2015) designed a two-factor authentication scheme and they use a dynamic ID-based technique that eliminates all constant parameters from the user's messages such that any two messages are independent and indistinguishable. Chang et al. (2015) claim their proposed smart-card-based two-factor authentication can achieve user anonymity and resist attacks like impersonation attacks, stolen verifier attacks, and lost smart card attacks. Islam et al. (2014) and Cao and Zhai (2013) also argue that the dynamic ID technique can enhance system security. Unfortunately, none of the above articles discloses empirical tests of their authentication systems, e.g., using simulations or experiments. It is unknown how their authentication would work in an actual work situation.

Demanding Computer Power and Operating Complexity: A one-time password token is another stream aimed at developing a possession-based two-factor authentication method. For this purpose, Cheng (2011) created a new cipher system called Rubbing Encryption Algorithm (REAL). This authentication system can generate a ciphertext REAL image, a type of one-time encrypted password. The user can decrypt the REAL by laying the hardware token over the REAL image on the screen (i.e., scan the token on the screen) to get the one-time password. The system does not

require the user to memorize the decryption key, so the REAL image can contain a long and complicated encryption key that enhances the overall system security. In addition, the authors claim that REAL does not use a complicated mathematic operation. It only requires a small level of computing power to operate the system, so it can also reduce the implementation cost. In addition, Y. Ku et al. (2013) use a graphical one-time password technique to create two-factor authentication to protect users from shoulder surfing attacks, man-in-the-middle attacks, and other phishing attacks. Their authentication method utilizes users' memory by implementing a story-telling mechanism in which users are required to create a *pass* image portfolio, and users need to identify the pass images from among fake images before entering the next authentication process. However, the authors did not provide any empirical evaluation in their study. The superior performance of their proposed authentication scheme is yet to be established.

3.4.3 Theme 3. User-Centered Weaknesses in Authentication Factors

The reliability of a security system can depend on the weakest node(Anderson & Moore, 2006), and relying exclusively on technology-based solutions is seldom enough to protect the organizational-digital assets (Bulgurcu et al., 2010). When the proposed new security systems increase the complexity of the existing security system, users are less likely to use or try two-factor authentication (Albayram et al., 2017). Thus, when designing a new two-factor authentication system, the researchers also need to balance the additional security afforded by the new system and the decrease of convenience caused by the system, resulting in user-centered weakness. In the following sections, we will discuss the more recent two-factor authentication system that focuses on improving users' experiences while using the system and its associated compromises.

Trust and Security Trust is always one of the main factors for users' IT adoption decisions. When using the information system, many users show privacy and security concerns and hesitate to use

information systems, especially when the system is used to handle sensitive information, such as medical information and bank transactions. Kassim, T, et al. (2021) found that two-factor authentication's security factor and effectiveness can increase customer trust when using internet banking, resulting in increased intention. However, while users want to see the enhancement of the new two-factor authentication practices, Kassim, T, et al. (2021) has shown that users' perceived authentication has no impact on customer trust. That means that users are less likely to care about which type of two-factor authentication the bank plans to implement. In addition, Tsai and Su (2021) suggest that two-factor authentication might be inadequate for protecting users against a takeover by cyber criminals, and multi-factor authentication is necessary to provide an extra layer of protection to secure customer accounts. However, they also point out that multi-factor authentication leads to barriers to adoption. That is the higher cost of deployment and maintenance and more complex integration between the authentication process and existing information, causing the regular users and the organization to hesitate to use more than two factors for authentication mechanisms.

Adoption Cost and Security Another important factor that influences IT adoption is its cost. The existing studies have found that users and organizations are less likely to adopt the information system when the adoption cost is higher. To address the adoption cost, Elshamy et al. (2021) designed two types of two-factor authentication systems to compare the costs and benefits of the designed system in the context of voice over the internet. Their study compares dual biometric factors (i.e., voiceprint and fingerprint) based authentication system with a password-and-voiceprint based authentication system. They found that the password-and-voiceprint-based authentication system is more cost-effective than the dual biometric factors-based authentication system because it does not require a fingerprint scanner to function. However, the simulation

results show that a dual-biometric factors-based authentication system is more secure than password-and-voiceprint due to the high accuracy of the fingerprint scanner. In addition, another stream of literature aims to design the new two-factor authentication system to minimize the use cost of regular users. Indeed, using ownership as an authentication metric has inherent advantages compared with other authentication mechanisms because it can verify the user with minimum or no user input(C. Wang et al., 2020). For instance, Čapek and Hub (2021) designed a two-factor authentication system that uses keystroke dynamics as the second factor besides the password. In short, the proposed keystroke dynamics authentication is a behavioral biometric authentication method that verifies patterns of keyboard users through their typing habits. Compared with other two-factor authentication systems that use keystroke dynamics, Čapek and Hub (2021)'s proposed system only requires a very small sample input from users. However, the proposed two-factor authentication system can only filter out 30% of intruders without mistakenly rejecting a single valid user. In comparison, Nguyen and Memon (2018) proposed a new two-factor authentication method using a smartwatch. Their proposed authentication mechanism can achieve an accuracy of 98.7% with a False Positive Rate of only 0.98%. Nguyen and Memon (2018) proposed an authentication mechanism that requires password and tap dynamics. The user can tap their smartwatch to record a melody of tap dynamics, and the authentication mechanism will store the time domain and frequency domain of the user's tap dynamics. The proposed new authentication mechanism can achieve similar performance to password-and-pattern-based two-factor authentication, but the new mechanism can better against smudge and shoulder sniffing attacks because the dynamics of the tap are hard to be observed.

3.5 Discussion

This systematic literature review elaborates on previous research into two-factor authentication by focusing on the meaning of existing empirical research in the area of current practice. There is a predominant assumption that two factors will provide better security than one factor (Cheong et al., 2014; Connie et al., 2004; Kumari & Khan, 2014; Yang et al., 2008). However, the research literature shows that these second factors are as rife with weaknesses as passwords. They are often costly, complicated to use, and open new avenues for compromise. Based on our systematic literature review, we found there is no strong empirical evidence to support the argument that two-factor authentication can provide an effective IS security solution.

First, the effectiveness of two-factor authentication is hard to measure because of the inconsistent evaluation method found among all selected articles. Experiments, simulations, security analysis, and cryptanalysis are the most common approaches to evaluating authentication performance. Due to the fundamental difference in these evaluation methods and measurements, it is difficult to compare the performance of different authentication methods directly. There was insufficient data to determine which authentication method is better and under what conditions.

Second, there is no strong evidence to support the argument that two-factor authentication can mitigate the risks from human errors and hacker attacks. Adding additional factors can provide extra security layers, but this study finds that such additional factors can also bring a lot of unexpected risks. Also, none of the selected articles examined the performance of their proposed security scheme in real-world settings. The research results may be biased due to an underestimation of the complexity of human behaviors. For example, the smartcard-based authentication-based security solution requires the users to secure the smart card from loss and report the loss immediately. If the users fail to comply with the security policy, they would be

more vulnerable to security threats, especially where higher transaction allowances are allowed with a smartcard.

Finally, the results of our systematic literature review of two-factor authentication yield a litany of weaknesses in the available authentication factors. Most researchers are concerned about the ease of compromise in one or more of these factors. While much of the work aims to improve the security and reliability of these diverse authentication factors, it collectively raises questions about two-factor practices. In other words, are two weak factors really better than one strong one? Considering the additional cost (i.e., high computational cost and extra hardware) and low reliability (i.e., low type II error but high type I error), the answer is unknown, and the practice is questionable. Clearly, there may be circumstances where adopting two-factor authentication could well be misguided. It may introduce expensive, complex, user-unfriendly technologies that only deliver the illusion of improved security.

3.6 Implications for research

First, the current two-factor authentication literature lacks a consistent performance evaluation method. One possible cause of this problem is that we lack a predetermined standard that guides researchers in evaluating the performance of the proposed two-factor authentication systems. At a minimum, the researchers should report false-rejection rate and false-acceptance rate. In addition to that, the researchers should also evaluate the authentication processing types across various contexts (e.g., a lab environment vs. a field experiment) based on the suggested hardware requirements. In addition, we found that many selected articles did not compare the performance of their proposed two-factor authentication systems with other types of two-factor authentication systems. To better help the practitioners and other security researchers understand the security performance of the new two-factor authentication system, we suggest that future studies should

not only compare the new two-factor authentication system with the existing two-factor authentication system that uses the same combination of authentication factors but also with the authentication system that used a different combination of authentication factors.

Second, all the selected articles use either lab experiments or simulations as the sole research method. Lab experiments and simulations may underestimate the complexity of human behaviors. As the previous research points out, many organizations consider employees as the weakest link in information security (Bulgurcu et al., 2010). Due to the nature of the information security context, the organization may not allow the researchers to test the prototype of two-factor authentication on-site, and we recommend future research is needed that relies more heavily on experiments or simulations to evaluate the performance of these authentication systems consistently before conducting the field experiment. Experiments and simulation methods use empirical data to generate consistent measurements. Shadish et al. (2001) suggest that experimental results are more generalizable, and such methods are best for investigating causal effect phenomena. After the lab experiment and/or simulation, if possible, we recommend additional field experiments that examine the practical performance of two-factor authentication in real-world, naturalistic settings (Lincoln & Guba, 1985).

Last, the current stream of two-factor authentication research lacks diversity. First, the majority of the selected studies focus on adding an additional authentication factor to the first password. The information security literature, including those selected studies, seems to agree that password-based authentication systems are problematic due to their inherent behavioral risks (e.g., simple passwords or the same passwords for all accounts). We suggest that, instead of adding an additional authentication factor to the password, more future research should focus on replacing the password by using either a possession factor or an inherent factor, creating a password-free two-factor

authentication system. In addition, we find that most of the selected articles were concerned with smart card-based two-factor authentication, and this basis leaves uncertainty about the effectiveness of other kinds of two-factor authentication. From the available smart card-based, two-factor authentication-related research, we found that lost smart card risk is unavoidable. This lost smart card attack can make this kind of authentication very vulnerable. Thus, we recommend more diverse two-factor authentication studies in the future. Second, only one selected article used behavioral research methodology (i.e., a survey) to examine individual users' attitudes toward two-factor authentication. The current two-factor authentication lacks the diversity of research methodologies. We call for more studies that use behavioral methods or econometrics to examine how individuals and organizations adopt two-factor authentication into their daily work and operation activities and what is the actual impact of two-factor authentication on individual and organizational security performance.

3.7 Implication for practices

In this study, we are not claiming that the organization should avoid adopting two-factor authentication; instead, we are promoting the two-factor authentication research and adoption in general by identifying the potential security risks that could be embedded in the introduced second authentication factor, guiding future researchers to mitigate those risks by using more secure protocols and practices. We agree with the existing literature that the two-factor authentication system should be theoretically safer and more robust against security attacks because it requires a higher-level skill set for malicious hackers. However, I want to call practitioners' attention to the potential technical security risks due to the design "flaws" in the proposed two-factor authentications as identified in this study. If the organizations plan to adopt the two-factor authentication from the selected articles, they should first conduct a field test to check the security

performance and integration compatibility with the existing information security systems. In addition to that, the practitioners should not only rely on a technological solution to improve their organization's security performance, and behavioral solutions, such as information security policy and security training, should also be applied to address the authentication challenges.

3.8 Limitations

It is likely that there are other studies about two-factor authentication that we have not included. Both ABI/Inform and EBSCOhost are well-developed and comprehensive. While it is likely, that we have the most prominent studies, it is not exhaustive. For example, we did find some two-factor authentication studies that were mentioned in the selected articles but were not included in the search results. This study only included refereed journal papers that dealt with the artifacts comprising two-factor authentication. Survey papers, expert opinions, and conceptual papers were not included. Accordingly, the research findings may not reflect the entire literature on two-factor authentication. Third, this study is interpretive research. While both authors were involved in the development process, one author performed the systematic review, including article selection, coding, and evaluation. These research findings are subjective, not objective. Last, this study does not compare the severity of the security risks embedded in the introduced second authentication factor. Different types of second authentication factors should contain various risks that bring different levels of impact on the reliability of the authentication systems. Future literature reviews are needed that examine the impact differences of varying security risks on authentication system.

3.9 Conclusion

In this study, we conducted this systematic literature review by surveying the two-factor authentication research from the ABI/Inform and EBSCOhost database. We analyzed 55 studies

in detail. Among these 55 selected articles, smart cards and passwords are the most studied two-factor authentication schemes, followed by fingerprints, digital keys, gait recognition, face recognition, radio frequency identification, one-time-use passwords, and palm prints.

Implementing two-factor authentication can add additional security layers. However, it also brings additional risks and reduces system useability. Biometric-based two-factor authentication system does not require the users to carry a physical key or memorize a password, but this kind of authentication requires using and storing sensitive data. This inherent disadvantage makes the system very vulnerable to privacy threats. Also, the biometric features of the same subject cannot be extracted exactly the same way twice. The system must tolerate a certain level of noise in the data, requiring the system to have a higher tolerance for variance. This tolerance concomitantly results in low accuracy rates and high implementation costs. In contrast, smartcard-based authentication systems have very high accuracy rates, but if the smart card is lost or stolen, the system could be even less secure than a single-factor authentication system. Hackers can get the information stored in a smart card through side-channel attacks, making the system very vulnerable to impersonation attacks. Smart-card-based two-factor authentication systems struggle to distinguish legitimate access from malicious access. It makes the system less attractive for practical deployment.

This study investigated the efficacy of two-factor authentication. There is a definite lack of empirical evidence to support the assumptions that a two-factor authentication scheme delivers superior security compared to a strong single-factor scheme. There are several reasons for this finding. There is an important need to develop a universal authentication performance evaluation standard. The present constellation of diverse performance evaluation methods and measurements makes the various existing research findings difficult to compare. There are no research data that

deal with optimally-paired two-factor authentication designs. Instead, many selected articles used cryptanalysis and security analysis methods as a proof-of-concept for artifacts. These methods do not use empirical data, leaving their practical performance in real-world authentication systems unknown. It is unclear whether their findings are suitable for practical deployment.

For future research, the clear finding of the review is that we need to increase both the number and the quality of studies on two-factor authentication. Despite its widely-accepted assumption as an advanced security practice, few researchers have focused on two-factor authentication itself, instead focusing on particular factors: technologies like smart cards and fingerprint scanners. Future research on two-factor authentication will be not only important but critical for the security of the digital age.

Appendix A Studies included in this review

1. Albayram, Y., Khan, M. M. H., & Fagan, M. (2017). A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA) [Article]. International Journal of Human-Computer Interaction, 33(11), 927-942. https://doi.org/10.1080/10447318.2017.1306765
2. Aman, M. N., Basheer, M. H., & Sikdar, B. (2019). Two-Factor Authentication for IoT With Location Information. IEEE Internet of Things Journal, 6(2), 3335-3351. https://doi.org/10.1109/JIOT.2018.2882610
3. Arshad, H., & Nikooghadam, M. (2015). Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol. J. Supercomput., 71(8), 3163–3180. https://doi.org/10.1007/s11227-015-1434-8
4. Arshad, H., Teymoori, V., Nikooghadam, M., & Abbassi, H. (2015). On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems. Journal of Medical Systems, 39(8), Article 76. https://doi.org/10.1007/s10916-015-0259-6
5. Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E. (2006). Privacy preserving multi-factor authentication with biometrics Proceedings of the second ACM workshop on Digital identity management, Alexandria, Virginia, USA. https://doi.org/10.1145/1179529.1179540
6. Cao, T. J., & Zhai, J. X. (2013). Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. Journal of Medical Systems, 37(2), Article 9912. https://doi.org/10.1007/s10916-012-9912-5
7. Čapek, J., & Hub, M. (2021). KEYSTROKE DYNAMICS AUTHENTICATION USING A SMALL NUMBER OF SAMPLES. E+M Ekonomie a Management. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=edsoai&AN=edsoai.on1262992225&site=eds-live&scope=site&custid=gsu1 https://dspace.tul.cz/handle/15240/158183; E+M Ekonomie a Management, volume 23, issue: 4; https://dspace.tul.cz/handle/15240/158183
8. Chang, I. P., Lee, T. F., Lin, T. H., & Liu, C. M. (2015). Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks. Sensors, 15(12), 29841-29854. https://doi.org/10.3390/s151229767
9. Chaudhry, S., Naqvi, H., Shon, T., Sher, M., & Farash, M. (2015). Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems [Article]. Journal of Medical Systems, 39(6), 1-11. https://doi.org/10.1007/s10916-015-0244-0
10. Cheng, F. (2011). Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm. Mobile Networks and Applications, 16(3), 304-336. https://doi.org/http://dx.doi.org/10.1007/s11036-011-0303-9
11. Cheong, S. N., Ling, H. C., & Teh, P. L. (2014). Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system. Expert Systems with Applications, 41(7), 3561-3568. https://doi.org/10.1016/j.eswa.2013.10.060
12. Connie, T., Teoh, A., Goh, M., & Ngo, D. (2004). PalmHashing: a novel approach for dual-factor authentication. Pattern Analysis and Applications, 7(3), 255-268. https://doi.org/10.1007/s10044-004-0223-4
13. Elshamy, E. M., Hussein, A. I., Hamed, H. F. A., Abdelghany, M. A., & Kelash, H. M. (2021). Voice over internet protocol voicemail security system using two factor authentication and biometric prints with new efficient hybrid cryptosystem [Article]. Multimedia Tools & Applications, 80(7), 9877-9893. https://doi.org/10.1007/s11042-020-09986-0
14. Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. Journal of Intelligent Manufacturing, 25(2), 217-230. https://doi.org/10.1007/s10845-012-0669-y
15. Guma, A., Mussa Ally, D., & Anael Elikana, S. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures [article]. Future Internet, 12(160), 160-160. https://doi.org/10.3390/fi12100160

16. Guo, M.-H., Liaw, H.-T., Deng, D.-J., & Chao, H.-C. (2011). An RFID secure authentication mechanism in WLAN. Computer Communications, 34(3), 236-240. https://doi.org/https://doi.org/10.1016/j.comcom.2010.02.033
17. Gupta, B. B., Prajapati, V., Nedjah, N., Vijayakumar, P., El-Latif, A. A. A., & Chang, X. (2021). Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS) [Article]. Neural Computing & Applications, 1-26. https://doi.org/10.1007/s00521-021-06152-x
18. Gupta, P., & Dhar, J. (2016). Hash Based Multi-server Key Exchange Protocol Using Smart Card [Article]. Wireless Personal Communications, 87(1), 225-244. https://doi.org/10.1007/s11277-015-3040-8
19. Hoang, T., Choi, D., & Nguyen, T. (2015). Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme [Article]. International Journal of Information Security, 14(6), 549-560. https://doi.org/10.1007/s10207-015-0273-1
20. Hsieh, W.-B., & Leu, J.-S. (2014). A Robust User Authentication Scheme Using Dynamic Identity in Wireless Sensor Networks. Wireless Personal Communications, 77(2), 979-989. https://doi.org/10.1007/s11277-013-1547-4
21. Huang, J. W., & Hou, T. W. (2007). A cost-effective add-on-value card-assisted firewall over Taiwan's NHI VPN framework. Med Inform Internet Med, 32(2), 103-116. https://doi.org/10.1080/14639230601135497
22. Islam, S. K. H., & Khan, M. (2014). Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems [Article]. Journal of Medical Systems, 38(10), 1-16. https://doi.org/10.1007/s10916-014-0135-9
23. Jiang, Q., Ma, J., & Tian, Y. (2015). Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of Zhang et al [https://doi.org/10.1002/dac.2767]. International Journal of Communication Systems, 28(7), 1340-1351. https://doi.org/https://doi.org/10.1002/dac.2767
24. Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks [Article]. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2016.10.001
25. Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition, 37(11), 2245-2255. https://doi.org/https://doi.org/10.1016/j.patcog.2004.04.011
26. Jover, R. P. (2020). Security Analysis of SMS as a Second Factor of Authentication [Article]. Communications of the ACM, 63(12), 46-52. https://doi.org/10.1145/3424260
27. Juan, Q., & Xiao-Ling, T. (2014). Two-Factor User Authentication with Key Agreement Scheme Based on Elliptic Curve Cryptosystem [Article]. Journal of Electrical & Computer Engineering, 1-6. https://doi.org/10.1155/2014/423930
28. Kassim, N., Ramayah, T., & Shabbir, M. S. (2021). Battling COVID-19: The Effectiveness of Biometrics Towards Enhancing Security of Internet Banking in Malaysia. Int. J. Enterp. Inf. Syst., 17, 71-91.
29. Khan, M. K., Zhang, J., & Wang, X. (2008). Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos, Solitons & Fractals, 35(3), 519-524. https://doi.org/https://doi.org/10.1016/j.chaos.2006.05.061
30. Khan, S. H., Ali Akbar, M., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. Pattern Recognition, 48(2), 458-472. https://doi.org/https://doi.org/10.1016/j.patcog.2014.08.024
31. Kim, J., Lee, D., Jeon, W., Lee, Y., & Won, D. (2014). Security Analysis and Improvements of Two-Factor Mutual Authentication with Key Agreement in Wireless Sensor Networks. Sensors, 14(4), 6443-6462. https://doi.org/10.3390/s140406443
32. Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J.-H. (2013). Two-factor authentication system based on extended OTP mechanism [Article]. International Journal of Computer Mathematics, 90(12), 2515-2529. https://doi.org/10.1080/00207160.2012.748901

33. Kumari, S., & Khan, M. K. (2014). Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'. International Journal of Communication Systems, 27(12), 3939-3955. https://doi.org/10.1002/dac.2590
34. Lat, J. A. S., Bondoc, R. X. R., & Atienza, K. C. V. (2013). SOUL System: secure online USB login system. Information Management & Computer Security, 21(2), 102-109. https://doi.org/http://dx.doi.org/10.1108/IMCS-08-2012-0042
35. Ma, B., Wang, Y., Li, C., Zhang, Z., & Huang, D. (2014). Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. Multimedia Tools and Applications, 72(1), 637-666. https://doi.org/http://dx.doi.org/10.1007/s11042-013-1372-5
36. Malina, L., Dzurenda, P., Hajny, J., & Martinasek, Z. (2018). Secure and efficient two-factor zero-knowledge authentication solution for access control systems [Article]. Computers & Security, 77, 500-513. https://doi.org/10.1016/j.cose.2018.05.006
37. Mann, C., & Loebenberger, D. (2017). Two-factor authentication for the Bitcoin protocol. International Journal of Information Security, 16(2), 213-226. https://doi.org/10.1007/s10207-016-0325-1
38. Naser, M. A. U., Jasim, E. T., & Al-Mashhadi, H. M. (2020). QR code based two-factor authentication to verify paper-based documents [Article]. Telkomnika, 18(4), 1834-1842. https://doi.org/10.12928/TELKOMNIKA.v18i4.14339
39. Nguyen, T., & Memon, N. (2018). Tap-based user authentication for smartwatches [Article]. Computers & Security, 78, 174-186. https://doi.org/10.1016/j.cose.2018.07.001
40. Ntantogian, C., Malliaros, S., & Xenakis, C. (2015). Gaithashing: A two-factor authentication scheme based on gait features. Computers & Security, 52, 17-32. https://doi.org/10.1016/j.cose.2015.03.009
41. Pang, Y. H., Andrew, T. B. J., & David, N. C. L. (2007). Two-factor cancelable biometrics authenticator. Journal of Computer Science and Technology, 22(1), 54-59. https://doi.org/10.1007/s11390-007-9006-x
42. Pomputius, A. F. (2018). A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory [Article]. Medical Reference Services Quarterly, 37(4), 397-402. https://doi.org/10.1080/02763869.2018.1514912
43. Pranata, S., & Hargyo Tri, N. (2019). 2FYSH: two-factor authentication you should have for password replacement [Article]. Telkomnika, 17(2), 693-702. https://doi.org/10.12928/TELKOMNIKA.v17i2.9187
44. Ravanbakhsh, N., Mohammadi, M., & Nikooghadam, M. (2019). Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme [Article]. Multimedia Tools & Applications, 78(9), 11129-11153. https://doi.org/10.1007/s11042-018-6620-2
45. Sherali, F., & Falah, S. (2020). An Efficient Two Factor User Authentication and Key Exchange Protocol for Telecare Medical Information System [Article]. International Journal of Mathematics & Computer Science, 15(4), 1015-1027. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=a9h&AN=146233939&site=ehost-live&scope=site&custid=gsu1
46. Ting, S. L., & Tsang, A. H. C. (2013). A two-factor authentication system using Radio Frequency Identification and watermarking technology. Computers in Industry, 64(3), 268-279. https://doi.org/https://doi.org/10.1016/j.compind.2012.11.002
47. Tsai, C.-H., & Su, P.-C. (2021). The application of multi-server authentication scheme in internet banking transaction environments [Article]. Information Systems & e-Business Management, 19(1), 77-105. https://doi.org/10.1007/s10257-020-00481-5
48. Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends [Article]. Computer Networks, 170, N.PAG-N.PAG. https://doi.org/10.1016/j.comnet.2020.107118
49. Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity [Article]. Information Sciences, 321, 162-178. https://doi.org/10.1016/j.ins.2015.03.070

50. Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2016). 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. IEEE Transactions on Vehicular Technology, 65(2), 896-911. https://doi.org/10.1109/TVT.2015.2402166
51. Wei, J., Liu, W., & Hu, X. (2014). Cryptanalysis and Improvement of a Robust Smart Card Authentication Scheme for Multi-server Architecture [Article]. Wireless Personal Communications, 77(3), 2255-2269. https://doi.org/10.1007/s11277-014-1636-z
52. Xie, Q., Dong, N., Wong, D. S., & Hu, B. (2016). Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol. International Journal of Communication Systems, 29(3), 478-487. https://doi.org/https://doi.org/10.1002/dac.2858
53. Xie, Q., Hu, B., Tan, X., Bao, M., & Yu, X. (2014). Robust Anonymous Two-Factor Authentication Scheme for Roaming Service in Global Mobility Network. Wireless Personal Communications, 74(2), 601-614. https://doi.org/10.1007/s11277-013-1309-3
54. Yang, G. M., Wong, D. S., Wang, H. X., & Deng, X. T. (2008). Two-factor mutual authentication based on smart cards and passwords. Journal of Computer and System Sciences, 74(7), 1160-1172. https://doi.org/10.1016/j.jcss.2008.04.002
55. Yin, X., He, J., Guo, Y., Han, D., Li, K.-C., & Castiglione, A. (2020). An Efficient Two-Factor Authentication Scheme Based on the Merkle Tree [Article]. Sensors (14248220), 20(20), 5735. https://doi.org/10.3390/s20205735

References:

Albayram, Y., Khan, M. M. H., & Fagan, M. (2017). A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA) [Article]. *International Journal of Human-Computer Interaction*, *33*(11), 927-942. https://doi.org/10.1080/10447318.2017.1306765

Aman, M. N., Basheer, M. H., & Sikdar, B. (2019). Two-Factor Authentication for IoT With Location Information. *IEEE Internet of Things Journal*, *6*(2), 3335-3351. https://doi.org/10.1109/JIOT.2018.2882610

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610-613. https://doi.org/10.1126/science.1130992

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). WHEN DO IT SECURITY INVESTMENTS MATTER? ACCOUNTING FOR THE INFLUENCE OF INSTITUTIONAL FACTORS IN THE CONTEXT OF HEALTHCARE DATA BREACHES [Article]. *MIS Quarterly*, *41*(3), 893-A898.

Arshad, H., & Nikooghadam, M. (2015). Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol. *J. Supercomput.*, *71*(8), 3163–3180. https://doi.org/10.1007/s11227-015-1434-8

Arshad, H., Teymoori, V., Nikooghadam, M., & Abbassi, H. (2015). On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*, *39*(8), Article 76. https://doi.org/10.1007/s10916-015-0259-6

Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E. (2006). *Privacy preserving multi-factor authentication with biometrics* Proceedings of the second ACM workshop on Digital identity management, Alexandria, Virginia, USA. https://doi.org/10.1145/1179529.1179540

Bose, I., & Alvin Chung Man, L. (2019). Adoption Of Identity Theft Countermeasures And Its Short- And Long-Term Impact On Firm Value [Article]. *MIS Quarterly*, *43*(1), 313-327. https://doi.org/10.25300/MISQ/2019/14192

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness [Article]. *MIS Quarterly*, *34*(3), 523-A527.

Cao, T. J., & Zhai, J. X. (2013). Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*, *37*(2), Article 9912. https://doi.org/10.1007/s10916-012-9912-5

Čapek, J., & Hub, M. (2021). Keystroke Dynamics Authentication Using A Small Number Of Samples. *E+M Ekonomie a Management*.

Chang, I. P., Lee, T. F., Lin, T. H., & Liu, C. M. (2015). Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks. *Sensors*, *15*(12), 29841-29854. https://doi.org/10.3390/s151229767

Chaudhry, S., Naqvi, H., Shon, T., Sher, M., & Farash, M. (2015). Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems [Article]. *Journal of Medical Systems*, *39*(6), 1-11. https://doi.org/10.1007/s10916-015-0244-0

Cheng, F. (2011). Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm. *Mobile Networks and Applications*, *16*(3), 304-336. https://doi.org/http://dx.doi.org/10.1007/s11036-011-0303-9

Cheong, S. N., Ling, H. C., & Teh, P. L. (2014). Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system. *Expert Systems with Applications*, *41*(7), 3561-3568. https://doi.org/10.1016/j.eswa.2013.10.060

Connie, T., Teoh, A., Goh, M., & Ngo, D. (2004). PalmHashing: a novel approach for dual-factor authentication. *Pattern Analysis and Applications*, *7*(3), 255-268. https://doi.org/10.1007/s10044-004-0223-4

Cranor, L. F., & Buchler, N. (2014). Better Together: Usability and Security Go Hand in Hand. *IEEE Security & Privacy*, *12*(6), 89-93. https://doi.org/10.1109/MSP.2014.109

Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication [Article]. *Computers & Security*, *63*, 85-116. https://doi.org/10.1016/j.cose.2016.09.004

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, *61*, 656-666. https://doi.org/https://doi.org/10.1016/j.chb.2016.03.068

Elshamy, E. M., Hussein, A. I., Hamed, H. F. A., Abdelghany, M. A., & Kelash, H. M. (2021). Voice over internet protocol voicemail security system using two factor authentication and biometric prints with new efficient hybrid cryptosystem [Article]. *Multimedia Tools & Applications*, *80*(7), 9877-9893. https://doi.org/10.1007/s11042-020-09986-0

Fagan, M., & Khan, M. M. H. (2016). *Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice*. USENIX.

Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. *Journal of Intelligent Manufacturing*, *25*(2), 217-230. https://doi.org/10.1007/s10845-012-0669-y

Guma, A., Mussa Ally, D., & Anael Elikana, S. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures [article]. *Future Internet*, *12*(160), 160-160. https://doi.org/10.3390/fi12100160

Guo, M.-H., Liaw, H.-T., Deng, D.-J., & Chao, H.-C. (2011). An RFID secure authentication mechanism in WLAN. *Computer Communications*, *34*(3), 236-240. https://doi.org/https://doi.org/10.1016/j.comcom.2010.02.033

Gupta, B. B., Prajapati, V., Nedjah, N., Vijayakumar, P., El-Latif, A. A. A., & Chang, X. (2021). Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS) [Article]. *Neural Computing & Applications*, 1-26. https://doi.org/10.1007/s00521-021-06152-x

Gupta, P., & Dhar, J. (2016). Hash Based Multi-server Key Exchange Protocol Using Smart Card [Article]. *Wireless Personal Communications*, *87*(1), 225-244. https://doi.org/10.1007/s11277-015-3040-8

He, D., Kumar, N., & Khan, M. (2013). Anonymous two-factor authentication for consumer roaming service in global mobility networks [Article]. *IEEE Transactions on Consumer Electronics*, *59*(4), 811-817. https://doi.org/10.1109/TCE.2013.6689693

Hoang, T., Choi, D., & Nguyen, T. (2015). Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme [Article]. *International Journal of Information Security*, *14*(6), 549-560. https://doi.org/10.1007/s10207-015-0273-1

Hsieh, W.-B., & Leu, J.-S. (2014). A Robust User Authentication Scheme Using Dynamic Identity in Wireless Sensor Networks. *Wireless Personal Communications*, *77*(2), 979-989. https://doi.org/10.1007/s11277-013-1547-4

Huang, J. W., & Hou, T. W. (2007). A cost-effective add-on-value card-assisted firewall over Taiwan's NHI VPN framework. *Med Inform Internet Med*, *32*(2), 103-116. https://doi.org/10.1080/14639230601135497

Islam, S. K. H., & Khan, M. (2014). Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems [Article]. *Journal of Medical Systems*, *38*(10), 1-16. https://doi.org/10.1007/s10916-014-0135-9

Jiang, Q., Ma, J., & Tian, Y. (2015). Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of Zhang et al [https://doi.org/10.1002/dac.2767]. *International Journal of Communication Systems*, *28*(7), 1340-1351. https://doi.org/https://doi.org/10.1002/dac.2767

Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks [Article]. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2016.10.001

Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, *37*(11), 2245-2255. https://doi.org/https://doi.org/10.1016/j.patcog.2004.04.011

Jover, R. P. (2020). Security Analysis of SMS as a Second Factor of Authentication [Article]. *Communications of the ACM*, *63*(12), 46-52. https://doi.org/10.1145/3424260

Juan, Q., & Xiao-Ling, T. (2014). Two-Factor User Authentication with Key Agreement Scheme Based on Elliptic Curve Cryptosystem [Article]. *Journal of Electrical & Computer Engineering*, 1-6. https://doi.org/10.1155/2014/423930

Karen D. Loch, a., Houston H. Carr, a., & Merrill E. Warkentin, a. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding [research-article]. *Mis Quarterly*(2), 173. https://doi.org/10.2307/249574

Kassim, N., Ramayah, T., & Shabbir, M. S. (2021). Battling COVID-19: The Effectiveness of Biometrics Towards Enhancing Security of Internet Banking in Malaysia. *Int. J. Enterp. Inf. Syst.*, *17*, 71-91.

Kassim, N., T, R., Mohamad, W., & Shabbir, M. (2021). Battling COVID-19: The Effectiveness of Biometrics Towards Enhancing Security of Internet Banking in Malaysia. *International Journal of Enterprise Information Systems*, *17*, 71-91. https://doi.org/10.4018/IJEIS.2021040104

Khan, M. K., Alghathbar, K., & Zhang, J. (2011). Privacy-preserving and tokenless chaotic revocable face authentication scheme. *Telecommunication Systems*, *47*(3-4), 227-234. https://doi.org/http://dx.doi.org/10.1007/s11235-010-9314-2

Khan, M. K., Zhang, J., & Wang, X. (2008). Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. *Chaos, Solitons & Fractals*, *35*(3), 519-524. https://doi.org/https://doi.org/10.1016/j.chaos.2006.05.061

Khan, S. H., Ali Akbar, M., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, *48*(2), 458-472. https://doi.org/https://doi.org/10.1016/j.patcog.2014.08.024

Kiljan, S., Simoens, K., De Cock, D., Van Eekelen, M., & Vranken, H. (2016). A Survey of Authentication and Communications Security in Online Banking [Article]. *ACM Computing Surveys*, *49*(4), 61:61-61:35. https://doi.org/10.1145/3002170

Kim, J., Lee, D., Jeon, W., Lee, Y., & Won, D. (2014). Security Analysis and Improvements of Two-Factor Mutual Authentication with Key Agreement in Wireless Sensor Networks. *Sensors*, *14*(4), 6443-6462. https://doi.org/10.3390/s140406443

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J.-H. (2013). Two-factor authentication system based on extended OTP mechanism [Article]. *International Journal of Computer Mathematics*, *90*(12), 2515-2529. https://doi.org/10.1080/00207160.2012.748901

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J. H. (2013). Two-factor authentication system based on extended OTP mechanism. *International Journal of Computer Mathematics*, *90*(12), 2515-2529. https://doi.org/10.1080/00207160.2012.748901

Kumari, S., & Khan, M. K. (2014). Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'. *International Journal of Communication Systems*, *27*(12), 3939-3955. https://doi.org/10.1002/dac.2590

Lampson, B. (2009). Privacy and Security: Usable Security: How to Get It [Article]. *Communications of the ACM*, *52*(11), 25-27. https://doi.org/10.1145/1592761.1592773

Lat, J. A. S., Bondoc, R. X. R., & Atienza, K. C. V. (2013). SOUL System: secure online USB login system. *Information Management & Computer Security*, *21*(2), 102-109. https://doi.org/http://dx.doi.org/10.1108/IMCS-08-2012-0042

Lennartsson, M., Kävrestad, J., & Nohlberg, M. (2021). Exploring the meaning of usable security – a literature review. *Information & Computer Security*, *29*(4), 647-663. https://doi.org/10.1108/ICS-10-2020-0167

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry* Sage Publications.

Ma, B., Wang, Y., Li, C., Zhang, Z., & Huang, D. (2014). Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. *Multimedia Tools and Applications*, *72*(1), 637-666. https://doi.org/http://dx.doi.org/10.1007/s11042-013-1372-5

Malina, L., Dzurenda, P., Hajny, J., & Martinasek, Z. (2018). Secure and efficient two-factor zero-knowledge authentication solution for access control systems [Article]. *Computers & Security*, *77*, 500-513. https://doi.org/10.1016/j.cose.2018.05.006

Mann, C., & Loebenberger, D. (2017). Two-factor authentication for the Bitcoin protocol. *International Journal of Information Security*, *16*(2), 213-226. https://doi.org/10.1007/s10207-016-0325-1

Naser, M. A. U., Jasim, E. T., & Al-Mashhadi, H. M. (2020). QR code based two-factor authentication to verify paper-based documents [Article]. *Telkomnika*, *18*(4), 1834-1842. https://doi.org/10.12928/TELKOMNIKA.v18i4.14339

Nguyen, T., & Memon, N. (2018). Tap-based user authentication for smartwatches [Article]. *Computers & Security*, *78*, 174-186. https://doi.org/10.1016/j.cose.2018.07.001

Ntantogian, C., Malliaros, S., & Xenakis, C. (2015). Gaithashing: A two-factor authentication scheme based on gait features. *Computers & Security*, *52*, 17-32. https://doi.org/10.1016/j.cose.2015.03.009

Pang, Y. H., Andrew, T. B. J., & David, N. C. L. (2007). Two-factor cancelable biometrics authenticator. *Journal of Computer Science and Technology*, *22*(1), 54-59. https://doi.org/10.1007/s11390-007-9006-x

Pomputius, A. F. (2018). A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory [Article]. *Medical Reference Services Quarterly*, *37*(4), 397-402. https://doi.org/10.1080/02763869.2018.1514912

Pranata, S., & Hargyo Tri, N. (2019). 2FYSH: two-factor authentication you should have for password replacement [Article]. *Telkomnika*, *17*(2), 693-702. https://doi.org/10.12928/TELKOMNIKA.v17i2.9187

Ravanbakhsh, N., Mohammadi, M., & Nikooghadam, M. (2019). Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme [Article]. *Multimedia Tools & Applications*, *78*(9), 11129-11153. https://doi.org/10.1007/s11042-018-6620-2

Sarel, D., & Marmorstein, H. (2006). Addressing consumers' concerns about online security: A conceptual and empirical analysis of banks' actions. *Journal of Financial Services Marketing*, *11*(2), 99-115. https://doi.org/http://dx.doi.org/10.1057/palgrave.fsm.4760025

Schneier, B. (2005). Two-factor authentication: Too little, too late. *Communications of the ACM*, *48*(4), 136.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2001). *Experimental and quasi-experimental designs for generalized causal inference* [Bibliographies

Non-fiction]. Boston : Houghton Mifflin, 2002.

Sherali, F., & Falah, S. (2020). An Efficient Two Factor User Authentication and Key Exchange Protocol for Telecare Medical Information System [Article]. *International Journal of Mathematics & Computer Science*, *15*(4), 1015-1027.

Ting, S. L., & Tsang, A. H. C. (2013). A two-factor authentication system using Radio Frequency Identification and watermarking technology. *Computers in Industry*, *64*(3), 268-279. https://doi.org/https://doi.org/10.1016/j.compind.2012.11.002

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British journal of management*, *14*(3), 207-222.

Tsai, C.-H., & Su, P.-C. (2021). The application of multi-server authentication scheme in internet banking transaction environments [Article]. *Information Systems & e-Business Management*, *19*(1), 77-105. https://doi.org/10.1007/s10257-020-00481-5

Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends [Article]. *Computer Networks*, *170*, N.PAG-N.PAG. https://doi.org/10.1016/j.comnet.2020.107118

Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity [Article]. *Information Sciences*, *321*, 162-178. https://doi.org/10.1016/j.ins.2015.03.070

Wang, D., Zhang, X., Zhang, Z., & Wang, P. (2020). Understanding security failures of multi-factor authentication schemes for multi-server environments. *Computers & Security*, *88*, 101619. https://doi.org/https://doi.org/10.1016/j.cose.2019.101619

Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2016). 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. *IEEE Transactions on Vehicular Technology*, *65*(2), 896-911. https://doi.org/10.1109/TVT.2015.2402166

Wei, J., Liu, W., & Hu, X. (2014). Cryptanalysis and Improvement of a Robust Smart Card Authentication Scheme for Multi-server Architecture [Article]. *Wireless Personal Communications*, *77*(3), 2255-2269. https://doi.org/10.1007/s11277-014-1636-z

Xie, Q., Dong, N., Wong, D. S., & Hu, B. (2016). Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol. *International Journal of Communication Systems*, *29*(3), 478-487. https://doi.org/https://doi.org/10.1002/dac.2858

Xie, Q., Hu, B., Tan, X., Bao, M., & Yu, X. (2014). Robust Anonymous Two-Factor Authentication Scheme for Roaming Service in Global Mobility Network. *Wireless Personal Communications*, *74*(2), 601-614. https://doi.org/10.1007/s11277-013-1309-3

Yang, G. M., Wong, D. S., Wang, H. X., & Deng, X. T. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*, *74*(7), 1160-1172. https://doi.org/10.1016/j.jcss.2008.04.002

Yin, X., He, J., Guo, Y., Han, D., Li, K.-C., & Castiglione, A. (2020). An Efficient Two-Factor Authentication Scheme Based on the Merkle Tree [Article]. *Sensors (14248220)*, *20*(20), 5735. https://doi.org/10.3390/s20205735

Yoo, C., Kang, B.-t., & Kim, H. K. (2015). Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. *Multimedia Tools and Applications*, *74*(10), 3289-3303. https://doi.org/http://dx.doi.org/10.1007/s11042-014-1888-3

Chapter 3 Postscript

This study fails to find empirical evidence to support the argument that two-factor authentication can improve overall system security. The individual point in this study is whether or not to introduce a second authentication factor when we need additional security technology to mitigate the risks embedded in the users' chosen simple-and-poor passwords. A systematic review of studies of two-factor authentication was conducted, and 55 studies from ABI/Inform and EBSCOhost were analyzed. The review investigates what is currently known about the benefits and limitations of two-factor authentication and how additional authentication factors affect security risk in relation to security costs. We found no strong evidence to support the assumption that two-factor authentication has superior performance.

The general assumption when designing new technology artifacts is that the technology designers need to balance the costs and benefits of implementing new security technology (i.e., two-factor authentication in my study). This balance is necessary because the users are motivated to retain the same level (or more) of convenience when they need to use new security technology to protect their or organizational assets.

In Essay two, I find strong evidence that the added second authentication factor can bring many unexpected risks. The second authentication factor could cause system failure points by intruding potential system vulnerabilities into the authentication system, causing the authentication less reliable and diminishing the protection benefits of two-factor authentication systems.

Chapter 4 Preface

An online community is a virtual society in which the community members are not necessarily known or identifiable but share an overarching goal. Online communities' sustainability relies on the voluntary participation of members to create and co-create a pool of digital resources (e.g., knowledge, news, open-source software code, videos) that allow members and others to derive value benefits continuously. While the information technologies give online community members a high degree of freedom in collaborating and creating digital resources at an unparalleled scale and speed, it also leads to member excesses. Its members may excessively exercise such freedom by using the shared digital resources with little consideration for others, decreasing the community sustainability.

We are endeavoring to create and apply information technologies to create an inclusive and free digital world. The high accessibility afforded by the technology may motivate its members to free-ride others' efforts in sustaining the shared digital resource systems. Indeed, the online community literature has shown that better communication technologies may not fundamentally change individuals' rationality and can collectively cause irrational decisions from the perspective of the group.

This study responds to the theme by demonstrating the potential technologies-induced system weaknesses and failure points in online community members' self-regulated digital resource provision and appropriation. In this study, I aim to explain how to understand free riding in a free digital world and how the free-riding will influence the online community's sustainability.

Chapter 4. When digital equality creates inequality: making open digital resource systems sustainable

4.1 Introduction

An online community (OC) is a virtual form of society in which the OC members are not necessarily known or identifiable but share an overarching goal (Faraj et al., 2011; Mindel et al., 2018). With the rise of Web 2.0 communication technologies, many different online communities have been created that allow users to interact and collaborate to create and co-create content. These include discussion forums, social media, open-source software development, and peer-to-peer (P2P) sharing networks. Online communities rely on the voluntary participation of members to create and co-create a pool of digital resources (e.g., knowledge, news, open-source software code, videos) that allow members and others to derive value benefits (Butler, 2001; Faraj et al., 2011; Mindel et al., 2018).

Many online communities from the beginning of Web 2.0 are still active. Some, however, did not last. For example, Yahoo Answer, one of the longest-running Q&A OCs for global knowledge sharing, was permanently shut down on May 4, 2021, after 16 years of operation. Yahoo's open statement informs that a reduction in Q&A platform popularity led Yahoo to shift resources away from the platform to products that better serve its members. Internet Movie Database (IMDB) decided similarly in 2017 to disable its discussion board and private messaging system despite many users still enjoying using it; IMDB encouraged its 250 million monthly users to use its social media account as the primary platform for posting comments and communicating with editors and other users.

OCs are blessed and cursed by their high degree of freedom, digital communication technologies having given community users inherent flexibility to collaborate and create digital resources at an

unparalleled scale and speed (Faraj et al., 2011). OC stakeholders can, however, join, use and leave the system at will (Mindel et al., 2018). Such freedom is not limited to individual users. Still, it extends to platform producers who can commercialize the community, close it down or change participation policies, threatening the freedom of the individual user. Baidu TieBa was, for example, the most popular Chinese OC and had thousands of topic-based discussion forums. Baidu TieBa, however, in 2011 changed its participation policies from selective participation and posting to almost no threshold. It furthermore implemented a new membership system that grants privileges to paid users, that allow them to override some participation rules. The changes helped Baidu quickly boost its revenues and increase its monthly active userbase to 300 million, the userbase however fell to just 37 million by 2020. Many former users complain that the popularity of the platform attracts too much low-quality content and annoying advertisements. The new participation policies and membership hierarchy seem to also encourage people to free-ride the system (e.g., over-post and redundant posting just to earn rewards, and trolling to discourage others' participation). This resulted in a sharp drop in user experience.

We are endeavoring to create and apply communication technologies to make an inclusive and free digital world. The above examples, however, remind us of a seminal statement of Mancur Olson:

"*But it is not in fact true that the idea that group will act in their self-interest follows logically from the premise of rational and self-interest behaviors…… unless the number of individuals in a group is quite small, or unless there is coercion or some other special device to make individuals act in their common interest, rational, self-interested individuals will not act to achieve their common or group interests(Olson, 1971, p. 1)."*

Indeed, Butler (2001) suggests that digital communication technologies do not fundamentally change the problems that underlie the development of a sustainable social structure. Therefore, collective action problems (Olson, 1971) can exist in the digital world, particularly in large groups. Creating an exclusive and small digital world may solve the problems but runs counter to the meaning of the internet. Better communication technologies may not fundamentally change individuals' rationality and can collectively cause irrational decisions from the group perspective.

OCs rely on voluntary user participation to remain sustainable (Faraj et al., 2011; Mindel et al., 2018). Voluntary participation does not automatically mean that people do this for nothing (McLure Wasko & Faraj, 2005; Mindel et al., 2018). The system is, therefore, only sustainable when it allows its stakeholders, including regular users and platform owners, to continuously derive value benefits (Butler, 2001; Mindel et al., 2018). Digital resource systems become more valuable as accessibility (Hess & Ostrom, 2007) and community size increase (Butler, 2001). They, however, also create the conditions in which collective action problems can arise (Olson, 1971), such as free-riding. This, therefore, raises an interesting research question:

How can we understand free-riding in a free digital world? How will free-riding influence the online community's sustainability?

It is worth noting that my use of decentralization reflects resource provision and appropriation (Mindel et al., 2018) and not a governance structure of power distribution (Tiwana, 2008). A decentralized digital resource system can have formal or self-regulated governance or even both (Faraj et al., 2015; O'Mahony & Ferraro, 2007)**.**

To answer my research question, I implemented a five-year ethnographic study of one of China's largest OC platforms. Ethnographers follow an abductive reasoning approach that generates

theoretical insights by encountering anomalies multiple times until a plausible and coherent solution evolves (Van de Ven, 2007). I began my research journey by drawing theoretical insights from the common-pool resource management literature (Hardin, 1968; Hess & Ostrom, 2007; Olson, 1971; Ostrom, 1990, 2009; Ostrom et al., 1994; Savas, 1977) and decentralized information systems literature (Butler, 2001; Faraj et al., 2011; Mindel et al., 2018). I then evolved and integrated these insights and findings with the service-dominant (S-D) logic (Lusch & Nambisan, 2015; Vargo & Lusch, 2004; Vargo et al., 2008). The common-pool resource system management literature is the theoretical context of my study and helps me frame and examine the problem through commons' perspective. Specifically, it (1) provides me with the initial understanding of how people interact with open resource systems, (2) helps me identify the boundary conditions of free-riding problems, and (3) helps me understand how free-riding can harm an open-sources system's long-term sustainability. The literature on decentralized information systems provides the unique contextual characteristics of the digital world, which can be taken into consideration when adapting the common management theories and examining free-riding problems in my digital ethnographic sites. I was finally able, with the additional help of S-D logic (Lusch & Nambisan, 2015; Vargo & Lusch, 2004; Vargo et al., 2008), to develop an understanding and interpretation of the findings on how the digital open resource system allows its users to co-create value through a services-for-services exchange and providing insights on sustaining the open resource systems.

The existing literature has provided many fruitful insights into the sustainability of open digital resource systems. It does, however, tend to examine the problem at the individual level, the main unit of analysis being user engagement. My study is, in contrast, heavily inspired by the commons management literature (Hardin, 1968; Olson, 1971; Ostrom, 1990), which focuses on examining

the incentives of open digital resource systems for free-riding, given the system's high degree of openness and stakeholders' rationality. The free-riding problem is, in this, a metaphor for a commons situation in which users fail to achieve collective benefits because of the conflict of interests that arises from people being motivated to maximize their immediate benefits instead of a greater long-term benefit as a group (Olson, 1971; Ostrom, 1990). Therefore, the free-riding problem is best interpreted as a system failure. The system's attributes and rules-in-use provide very little incentive for voluntary self-regulation or for user joint action to behave in the group's best long-term interests (Olson, 1971; Ostrom, 1990).

I organized the papers as follows. In the next section, I discuss the theoretical foundation, which is the management of the common-pool resources, that serves as my initial understanding of the open resource systems. In the second section, I describe the research approach and briefly introduce the social context of the study and my ethnographic investigation process. In the third section, I present the findings by illustrating how my initial understanding based on the existing literature on OCs and commons-pool resource system causes conflicts that challenge my initial understanding and how I resolve the conflicts by incorporating the theoretical insights from the S-D logic. In the last section, I provide a discussion of the findings and their broader implications for research and practices in managing open digital resources systems.

4.2 Theoretical Foundation

I first, to understand how individuals interact with the open resource system, discuss and distinguish three important concepts from the literature on the commons. These are commons, common property, and common-pool resources.

4.2.1 Commons, common property, and common-pool resource

In its simplest form, commons mean cultural or natural resources that are not owned by any individual but are accessible by all the members of the community. In other words, the resources are "held in common" (Anderies & Janssen, 2016). However, Commons, common property, and common-pool resource (CPR) should be treated as different concepts. Commons have, at the broadest level, both physical and institutional attributes. These are referred to as CPR, for example, groundwater and fish stocks, or common property such as pasture and public fishing grounds. Commons are, in terms of physical attributes, a type of resource that is used by a group of people (Hess & Ostrom, 2007), commons in the institutional term being institutionally arranged shared property (Godwin & Shepard, 1979) that is accessible, and with little or no physical and legal barriers. It is worth noting that the shared resources of common property can be public goods or CPR. The difference between the two is that the resources available to others are not reduced by the use of public goods but are by the use of CPR. In recent developments in commons literature, Commons is also applied to the public intellectual domain (Hess & Ostrom, 2003) or the digital domain (Mindel et al., 2018). The public intellectual domain indicates that commons can be about the democratic process, freedom of speech, and the free exchange of information (e.g., scholarly journals).

Similarly, the digital domain defines commons as a digital commons, a highly accessible and self-selected digital platform on which users exchange, create and co-create digital content. For example, Mindel et al. (2018) define the information commons as "a *highly accessible, self-rising information system in which stakeholders share an overarching goal*" (p.609). The OC property of high accessibility indicates that the information commons are generally non-exclusive, meaning that the individual can freely join and leave the community without any spatial or temporal

limitations. Opposing the top-down influence mechanism, the OC is a self-rising property that reflects how the OC is inherently evolutionary (Mindel et al., 2018). The individual interactions shape the community's resources, characters, and capabilities (Thompson, 2005).

4.2.2 Free-riding problems and their origin

Ostrom (2009) suggests that "*all humanly used resources are embedded in complex, social-ecological systems* (Ostrom, 2009, p. 419)." The social-ecological system's subsystems, which include the resource system, resource unit, governance system, and users, are relatively independent but interact to produce either positive or negative collective outcomes (Ostrom, 2009). Due to its high degree of openness, a commons could create behavioral incentives for individuals to free-ride (Hess & Ostrom, 2007; Ostrom, 1990; Ostrom et al., 1994), free-riding in the simplest form, meaning that someone uses the resources without bearing its obligated costs. Free-riding becomes a common's problem when its users cannot exclude and be excluded by others, and each individual is motivated to free-ride others' efforts to sustain the system.

One of the first scholars to focus their attention on free-riding problems is Gordon (1954). Gordon (1954) demonstrated that in a commons-owned fishery resource, fishers race to harvest as many fish as possible until the marginal benefit of catching additional fish equals the marginal cost of harvest. The number of fish harvested would, therefore, quickly exceed the maximum sustainable yield (i.e., fish appropriation is higher than provision) and economic yield (i.e., fish supply is greater than market demand). Hardin (1968) later crystallizes this idea in this stream of literature by using the metaphor of the tragedy of the commons. Hardin illustrates the common's dilemma through the herder problem, in which a rational herdsman who wants to maximize his gain always asks himself, "*what is the utility to me of adding one more animal to my herd? (Hardin, 1968, p. 1244)*". Many herders share a pasture. Adding animals to his herd, therefore, increases his proceeds

from the sale of the additional animals. The cost of overgrazing, however, is shared across all herders. The dominant strategy in the herder's problem is always the strategy that adds more animals to the public grazing land and acts faster. Herders on a shared pasture are, for two reasons, therefore locked into the path to tragedy. First, the pasture will soon reach its environmental capacity, with more animals causing pasture depletion and even destroying the entire ecosystem. Second, rational herders cannot solve the problem on their own. As Hardin argues, the only solution to the commons problem is an external authority, such as a government, that allocates resources at a renewable rate, monitors commons use and punishes noncompliance.

Not all commons can, however, afford and/or are willing to accept an external authority due to administration costs, sanction reliability, monitoring capability, and accuracy of information (Ostrom et al., 1994). Ostrom found, through multiple empirical studies, that many but not all commons can save themselves from tragedy without an external authority (*e.g., Ostrom (1965)*), the findings challenging the tragedy of the commons assumption (Hardin, 1968), which is that people in commons cannot self-regulate and achieve a long-term goal as a group. In her 1990 seminal book "Governing the Commons, " Ostrom summarized findings of how a number of polycentric principles governing commons could be applied to avoid resource overexploitation. The selected polycentric governance principles include clearly defined boundaries, collective choice arrangement and graduated sanctions.

In conclusion, common-pool resource management literature is the ideal candidate for providing the theoretical foundation to examine OC's sustainability issues for two main reasons. First, OC can be viewed as an open resources system (Butler, 2001; Mindel et al., 2018). When the resource system opens to all, collective action problems are unavoidable (Olson, 1971). The existing OC literature has identified that the OC can face sustainability challenges due to the community size

increase (Butler, 2001), dynamic change in resources (Faraj et al., 2011), and collective action threat (Mindel et al., 2018), etc. Thus, the open digital resource system could create inherent tension between maximizing individual OC members' participation benefits and retaining the sustainable social-technical structure that achieves the community's long-term group interests. Second, we may use different theoretical perspectives to examine the OC sustainability issues. However, the common-pool resources literature can provide unique and comprehensive theoretical angles that examine the OC sustainability issues, focusing on commons' resource provision and appropriation. Indeed, free-riding, which is the focus of this study, can originate from the resource provision side or the resource appropriation side (Ostrom et al., 1994). Appropriation means that system users withdraw/use resource units from the system. Provision is the opposite and focuses on the maintenance of a resource unit's supply and system. The resource flow is the problematic element for a commons with an appropriation problem, the yield of resource units between production and consumption being unbalanced. The commons' resource facility or resource stock is the problematic element for commons with a provision problem, the commons having difficulty creating resource units, improving resource production, or avoiding system destruction. Therefore, I argue that commons-pool resource literature is the ideal candidate for me to understand the free-riding problems arising from both digital resource provision and appropriation sides.

4.3 Research Method

To answer my research questions, I conducted a five-year ethnographic study at Autohome.com from October 2017 to March 2022. I employed ethnographic methods, which have shown to be useful for exploratory study and in studying novel information system phenomena(Schultze, 2000; van den Broek et al., 2021). Thus, the ethnography methodology is an excellent fit for me to answer my research questions.

Agar (1986) describes the ethnographic process as a movement from breakdowns to establishing a coherent understanding of the focal phenomena that challenge the ethnographer's assumption. Ethnographers need a language to describe and evaluate their studies if they are to enhance the quality of research findings and increase generalizability (Agar, 1986a). I, in this study, adopt the Agar (1986a) ethnographic multiple-strip resolution from the interpretivism paradigm to guide us in the design of this study and the organization of the findings. The primary work on the method (Agar, 1986b) is widely cited (2163 citations in Google Scholar) and has been applied or adapted in many other disciplines; examples include, Anthropology (e.g., Agar & Hobbs, 1985), Computer Supported Cooperative Work (e.g., Hellmann et al., 2016), Education (e.g., Jaffe-Walter, 2020), Law/Criminology (e.g., Wettergren & Bergman Blix, 2016), Medicine (e.g., Hsu et al., 2017), Organizational Studies (e.g., Le Trividic Harrache, 2017), and Psychiatry (e.g., Kovarsky, 2016).

Multiple-strip resolution consists of multiple single-strip resolutions. A single-stripe resolution is formed by three elements: *schema, strip, and breakdown* (Agar 1995). Schema is the ethnographer's initial understandings and expectations of the reality they are coming from or anomaly the ethnographer encountered and wants to understand (Van De Van 2007, Agar 1995). The strip is how the ethnographer's construct encounter(s) with people in reality that help ethnographers to collect data and understand the focal culture. Agar suggests that ethnographers should apply themselves as research instruments to facilitate encounters with focal folks that "*show how social action in one world makes sense from the point of view of another (Agar, 1986a)*." The units that construct the strip are not limited by any form, for example, observation, interview, conversation, and experiment. The breakdown is the difference between the ethnographer's expectation of reality and the actual reality observed. Once a breakdown occurs, we have a *schema problem* that requires ethnographers to make *plausible* inferences and propose a new schema until

all breakdowns disappear. Ethnographers, in reality, may have to implement a multiple-strip resolution that applies a series of single-strip resolutions to achieve an ethnographic understanding.

The output of multiple-strip resolution is ethnographic understanding (Agar, 1986a). Ethnographic understanding will occur "*when the horizons of the different traditions have been fused – changed and extended so that breakdown disappears (Agar, 1986a, p. 21)*". An ethnographic understanding of the differences between studied realities and experienced realities can enable ethnographers to bridge the gap between so-called weakly connected paradigms. Ethnographers may encounter people in focal cultures multiple times until anomalies or problems of interest have been resolved and a coherent understanding is achieved. Agar (1986a) suggests that ethnographic understanding should meet three criteria. First, ethnographers need to explain why the current ethnographic understanding is better than other resolutions that can be imagined and why there is no need to propose additional strip resolutions. The second is that ethnographers need to connect ethnographic understanding to a broader knowledge, which constitutes a tradition. Lastly, ethnographic understanding aims to elicit an "aha" reaction from people from different traditions.

4.3.1 Ethnographic Sites and Data Collection

This ethnographic study is colored by my more than ten years of personal experience as a car enthusiast who actively participates in multiple automotive discussion-forum-based OCs. The study itself is the result of more than four years of fieldwork between 2017 and 2021 on AutoHome.com (See table 1 for data collection summary). AutoHome defines itself as the leading online destination for the automobile consumer in China. My ethnographic sites are multiple discussion forums on the AutoHome website and a number of discussion groups created by AutoHome community users.

Kozinets (2002) suggests, when selecting suitable OCs for investigation, that "*online communities should be preferred that have (1) a more focused and research question-relevant segment, topic, or group; (2) higher "traffic" of postings; (3) larger numbers of discrete message posters; (4) more detailed or descriptively rich data; and (5) more between-member interactions of the type required by the research question.* (Kozinets, 2002, p. 63)." AutoHome OC satisfies the above criteria well. AutoHome had, when I started my study of AutoHome's OC in 2016, more than 21 million daily active users in over 1,400 topic-based discussion forums. AutoHome also was the most active automobile consumer OC in China, creating discussion forums for almost every single make and model of car on China's market.

Table 4-1. Overview of Data Collection

Period	Data Type	Data Details
October 2017 to September 2019	Passive observation	Weekly visited the following AutoHome discussion forums: Volkswagen CC forum, Mercedes S Class forum, Elite-Homepage Threads forum
December 2019 to June 2020	Participant observation	Daily visited Tesla Model 3 discussion forum. Created 70 original threads and received over 2,500 replies and over 300,000 views.
September 2019 to March 2020	Passive observation	Daily visited NIO ES6 discussion forum
November 2019 to March 2022	Passive observation	Joint 4 Tesla and 4 NIO discussion groups
May 2021	Structured Interview	Conducted 18 interviews with platforms editors
July 2021 to November 2021	Multiple-rounds semi-structured Interview	Conducted 21 interviews with 10 platform managers and editors
January 2022 to March 2022	Passive Observation	Weekly visited Tesla Model 3 discussion forum

I used online participation, including passive observation, participant observation, and unstructured and semi-structured interviews, to explore how OC stakeholders, including AutoHome regular users and platform hired editors, interact and derive value benefits from the

community open-source system (i.e., discussion forum). Online participation allowed me to observe the focal OC activities in an entirely unobtrusive way, to observe individuals' behavior naturally, and minimize any researcher-induced demand effects (Kozinets, 2002, 2010). Such online observation-based research will also bring unexpected challenges in avoiding violating the right of individuals, including privacy concerns and unexpected manipulation due to my participation. I have, therefore, combined the guidelines suggested by Kozinets (2010) and my Institutional Review Board (IRB), strictly followed the IRB's guidelines, and carefully reviewed the user agreement of AutoHome, to ensure my participation does not violate its policies. I also used secondary data to validate the ongoing research findings and discover and resolve breakdowns that helped me achieve ethnographic understanding. The South China University of Technology makes this secondary data available to me. It consists of deidentified, summarized data sets from interactions with other online community editors from a similar automobile consumer social media platform.

4.3.2 Ethnographic Investigation Procedures and Data Analysis

Resolution 1. Searching for online community resources

My first single-strip resolution started in September 2016 and ended around April 2018. This resolution cycle aimed to understand OC sustainability based on individual users' perspectives, the focus being on content provider disengagement. The ethnographic sites included the Elite Homepage Threads forum, Volkswagen CC forum, and the Mercedes-Benz S-Class forum. I used passive observation to construct the strip in this stage. I, therefore, did not interact with any AutoHome users or create any threads. However, I regularly visited the above-mentioned forums and summarized the findings in fieldnotes.

I selected these forums by following Kozinets (2002) suggestions: higher posting "traffic", relevant to initial research interests, and a larger number of discrete message posters. All three forums were very active. I believed that it was likely that I would observe a conflict of interests between content providers and other community users in these forums that caused content providers to disengage from participating in community activities.

Agar suggests that when an ethnographer's expectations of reality are different from the actual reality observed, we have a breakdown problem that must be further addressed by proposing a new resolution cycle. My first schema is the common-pool- resource management literature, as discussed before. Two interesting phenomena challenged my initial expectations of content provider disengagement in this stage of data collection. First, I observed an increasing number of content providers try to regain ownership of the content they had created and the discussion forum, for example, by repeatedly expressing statements such as "This is my territory," "This place belongs to true car enthusiasts," or "No one asks you to read if you don't like, just leave." Some content providers, when threads attracted too much-unwanted attention and replies, "*deleted*" not just one but all their previous threads, including those that had received Elite Homepage Content Recognition. I was surprised by such members withdrawing because, with over 21 million daily active users but less than 100 recognitions available per day, it is extremely difficult to achieve Elite Homepage Content Recognition which is the highest reward that could be given to the threads. Users must spend hours or even days creating a thread that is good enough to earn this award. AutoHome does not, however, allow users to delete but allows users to edit their threads. Many users, therefore, changed their threads to blank to "*delete*" them. I found, when I closely examined previous replies of disengaged content providers, that many mentioned that the forum discussion environment was being ruined by keyboard drivers, paid reviewers, and distractors (similar to

internet trolls). I presented my initial findings at the ICIS 2018 conference in the middle of this phase of data collection to get feedback from the academic community, which helped me design the data collection for the next stage (Wang, 2018).

In the later phase of the investigation, I narrowed my observation to high-profile and new contributors who deleted their high-quality threads. I found that some still visited the discussion forums but no longer created any additional threads and only rarely replied to other community users. The initial findings were presented at the 2019 PACIS conference (Wang & Baskerville, 2019).

Resolution 2. Experiencing online community's commons problem

My overall researcher interests were unchanged when starting the second single-strip resolution cycle. I still aimed to explore OC sustainability challenges. However, I realized that I would never achieve ethnographic understanding if I continued to investigate as a passive observer and limited my focus by just understanding individual user behaviors.

My second resolution cycle started on two forums in September 2019 and ended in October 2020: the NIO ES6 forum and Tesla Model 3 forum. I selected these two forums for the following reasons. When I started my observation, both forums were recently created and had not been appointed forum moderators. This provided a perfect window of opportunity to observe forum users' self-regulated behavior. Second, adopting electric vehicles is becoming a major trend in China. I, therefore, believed that an increasing number of users would join the forums during the investigation. Free-riding problems tend to be more severe in a larger community (Olson 1971; Ostrom 1990). The membership size dynamic allowed me to examine how membership size influences free-riding behavior, if any. Lastly, I intended to participate as a registered car owner on the Tesla Model 3 forum. My participation may, however, unintentionally have caused

researcher-induced demand effects. I, therefore, also passively observed the NIO ES6 forum and used it as a reference community to further understand how my participation may or may not influence the focal community culture. The NIO ES6 forum could be my best reference community candidate because it is a direct competitor of Tesla, and both forums share a similar userbase. I found that many OC users participated in both forums before and during my second resolution cycle.

Starting in September 2019, I first passively observed forum activities on the NIO ES6 forum and Tesla Model 3 forum for about four months, stopping my daily passive observation of the NIO ES6 forum when the forum formally appointed a forum moderator. As a registered car owner, I actively participated daily on the Tesla Model 3 forum from December 2019 while regularly visiting the ES6 forums as an observer. I created 70 original threads on the Tesla Model 3 forum in the 13 months of data collection in stage 2, which resulted in over 2,500 replies and over 300,000 views. Five of the 70 original threads were awarded elite content, one being awarded an Elite Homepage Content Recognition. At the end of my second data collection stage, I was ranked as a top 10 contributor of 21,000 registered users. My high level of contribution to the Tesla Model 3 Forum and expertise in electric cars resulted in me being encouraged by Tesla China marketing officials and many Model 3 forum users to apply for the forum moderator position.

I also found, during my investigation, that many Model 3 and ES6 forum users, both registered users and lurkers, use other platforms (e.g., WeChat, Zhihu-Chinese Quora, and Weibo- Chinese Twitter) to exchange and gather information. These cross-platform user experiences could help me understand whether platform attribute differences cloud influence free-riding behavior. I, therefore, joined 8 WeChat chat groups created by AutoHome users from ES6 and Model 3 forums to seek additional insights. Each chat group had around 300 to 400 participants, many being AutoHome

forum lurkers without AutoHome accounts but who regularly visited the forums to read shared content. My interactions with these WeChat group users were summarized into fieldnotes for further analysis. Lastly, I conducted email interviews with 18 rival platform media editors to resolve some of the breakdowns and better understand how the company operates and manages the discussion forums. The media editors had, on average, 2-3 years of working experience in operating and managing discussion forums.

Resolution 3. Examining the online community sustainability challenges through the eyes of platform editors

My last single-strip resolution started in September 2021 and ended around March 2022. I interviewed 16 automobile social media platform editors and five AutoHome platform editors and managers in this study phase. During this investigation phase, I first had a two-hour phone interview with the AutoHome platform manager using semi-structured interviews. The interview focused on his experience and difficulties when he managed the OC discussion forums. I also asked for feedback regarding my pre-determined interview questions. After the interview, I re-designed the interview questions and was referred to four AutoHome discussion forum editors to conduct further interviews. Due to time zone differences and schedule conflicts, I sent the pre-determined interview questions as open-ended surveys to the forum's editors through Qualtrics. After reviewing and analyzing their answers, I conducted follow-up interviews with each editor by using WeChat. In addition, I followed the same approach to conducting an additional five interviews with other Automobile social media platform editors who have an average of 2-3 years of experience managing Automobile discussion forums. I also added those editors to my WeChat contact list to have a follow-up interview and discuss additional insights during data analysis. At the end of each interview, the interviewees received ¥100 RMB as compensation.

In the last resolution cycle, I aim to achieve the ethnographic understanding by sharing and re-interpreting my findings with the platform editors. The main purpose of this phase of the investigation is to validate my findings. Klein and Myers (1999) suggest that contextualization is one of the key principles for interpretive research. Contextualization requires that " *the subject matter be set in its social and historical context so that the intended audience can see how the current situation under investigation emerged. (Klein & Myers, 1999, p. 73)"* Thus, during my interpretation, I explain why online communities can be viewed as a commons while considering the contextual characteristic of my focal OCs platform based on my previous observations. In addition, I interpret my findings by following the hermeneutic cycles. Hermeneutic cycles suggest that "*all human understanding is achieved by iterating between considering the interdepending of parts and the whole that they flow(Klein & Myers, 1999, p. 72)."* I iteratively analyzed my data for anticipated emergent themes, then tacked back and forth repeatedly between my understanding of the problems and new insights generated from interactions with the platform editors and managers. I interpret the findings by iterating between the individual AutoHome stakeholders' participation, including ourselves, and the global context of the whole platform that determines the full meaning of the individuals' participation and its influence on the OC's sustainability.

The result of all three resolution cycles and data analysis was a large dataset of about 2.28 GB containing over two hundred pages of field notes, hundreds of downloaded threads, 39 interview reports from automobile media editors, thousands of WeChat interactions, and hundreds of photos and few videos that I used to create my threads.

To analyze threads and my interactions with AutoHome users, I imported all downloaded threads and WeChat interactions to NVivo at the beginning of the study. However, I soon realized that the data I collected had too much "noise" and was too large, which might not be useful for

understanding the focal culture, causing barriers for me to interpreting the findings. During the middle of the investigation, I summarized my daily observation into fieldnotes, and my interpretation of my interaction with AutoHome users was mainly based on my daily fieldnotes.

4.4 Findings

4.4.1 Online community open-access resources system

This section explores AutoHome online communities as an open-access resource system and its contained resources. Ostrom (1990)classifies resources into four categories based on two attributes: excludability and rivalrous (see Table 2). The excludability attribute focuses on the ownership of the resources, and highly excludable resources mean that the members can exclude and prevent others from using the same resource system. The rivalrous attribute focuses more on the resource's characteristics. Rivalrous resources mean that resources being used by one member will simultaneously prevent others use the same resources. In other words, the consumption of one resource unit reduces the ability of others to consume it. Under this classification system, there are four types of resources: public goods resources that are non-excludable and non-rivalrous (e.g., public roads and open-source software), private goods resources that are excludable and rivalrous (e.g., foods and cars), club goods resources that are excludable but non-rivalrous (e.g., golf club and toll road), and common-pool resources that is non-excludable but rivalrous (e.g., fish stock and pasture).

Table 4-2. Goods classified by exclusivity and rivalrous

	Low Excludability	**High Excludability**
Low Rivalrous	Public goods (e.g., public roads and air)	Clube goods (e.g., golf club and cinemas)

High Rivalrous	Common-pool resources (e.g., fish stocks and coal)	Private goods (e.g., food and cars)

The conventional wisdom seems to agree that online communities are formed by the public goods resources (i.e., digital resources) only as the unique characteristic of Web 2.0 is user-generated content compared with Web 1.0. For instance, information or user-generated content, including open source code and shared knowledge, are public goods resources as they are non-rivalrous and non-excludable and are being studied as the key resource for online communities (Faraj et al., 2011; Faraj et al., 2016; Mindel et al., 2018; Wasko et al., 2004). Other studies view namespace (i.e., common-pool resource) (Forte et al., 2009) and members' attention (i.e., private goods) (Shen et al., 2015) as the online communities' resources. I find the above studies only focus on one type of resource that influences the OC's sustainability but overlook the fact that even the public goods (e.g., public roads and open-access digital resources) need to be combined with other types of goods to produce the final service (Anderies & Janssen, 2016). For instance, a public road is meaningless without cars (i.e., private goods), some toll roads (i.e., club goods), and public buses (i.e., common-pool resources). Indeed, throughout my investigation, my ethnographic site, AutoHome online communities, is also a complex open resource system that involves not only one but many different types of goods to produce automobile services for its users (see table 3 for the summary).

Table 4-3. AutoHome Resources Classification based on Ostrom 1990

	Low Excludability	**High Excludability**
Low Rivalrous	AutoHome public goods: Platform IT infrastructure, digital contents	AutoHome club goods: Authome users' recognition (i.e., verified car owners, elite

		content, and homepage-elite content)
High Rivalrous	Common-pool resources: discussion forums' digital spaces.	Private goods: individual user's attention, knowledge before sharing.

My observation supports the view that AutoHome is a comprehensive digital media platform that aims to provide one-stop-shop services for Chinese automobile customers by offering offers four main types of digital services to its users: professionally produced content and online discussion forums, automobile library, and automobile listing information. Among those offered services, the discussion forum-based online community is a major part of the AutoHome platform. When I asked one of the AutoHome platform editors what role discussion forums play in the AutoHome business model, he answered:

"For AutoHome, the online forums are more like cisterns. If your website only has car news and product catalogs, they will just leave [after getting the needed info]. Without forums, AutoHome is nothing but a tool. With the forums, we can retain the customers so that we can leverage other values from the customers by finding their potential needs, such as car shopping, car maintenance, road trips advice." – Interview, Mr. Wu from AutoHome.

Mr. Wu's answer has shown that AutoHome users are not attracted by any single service or resources provided by AutoHome but by the multiple services afforded by the platform. Thus, an online community is like a conventional public goods resources-based system that requires multiple types of resources to produce its final services. In the following, I will discuss the types of goods afforded by the AutoHome platform for its online discussion forum users according to Ostrom's classification schema based on my observation.

AutoHome's discussion based on OC is a public platform that can be accessed by all its users who may or may not have a registered account. Thus, the platform infrastructure can be viewed as a public goods resource as it is non-excludable and non-rivalrous. A registered account is not required to use the forums, but an account is required to create content (e.g., threads, replies, and car reviews). Registered AutoHome users can participate in any forum activities. They will be shown as a specific forum registered user if they have voluntarily indicated their interests in any car or registered their car ownership through the platform verification system. When creating and replying to threads, a registered car owner will have a special digital status badge beside their avatar that shows them to be a verified car owner.

The AutoHome platform contains a registered car owners club to distinguish regular users and car owners further and retain its users. The car owners club inside the AutoHome platform is a club goods resource as it only allows real car owners to join the club, but there is no upper limit on the number of club members. A forum user can verify car ownership by registering their car through the AutoHome verification system and uploading a valid driver's license and car registration. AutoHome also allows users to register ownership manually. The user can create a discussion thread to prove their ownership by uploading photos of the car and key or car registration license. They can then message the forum moderator or email the platform editor team to update their car ownership status manually.

AutoHome user participation is voluntary, which aligns with the high-accessible commons with a high degree of freedom (Mindel et al., 2018). When creating content, users can choose the type of content - regular discussion thread or video clip. Users can voluntarily indicate the type of regular discussion thread, such as questions, user experience, travel log, and repair & maintenance. The forum has, where content is not classified, a fairly accurate algorithm that can automatically

classify content that allows other users to filter. The system functions for video clips are similar to those of a regular video platform, such as YouTube. The system allows users to create a short description and allows others to comment on the videos, uploaded videos being shown in the same shared place as regular discussion threads. During my observation period, the platform gave users higher incentives to upload video clips, such as a higher amount of reward points. The majority of users still, however, preferred to communicate via conventional discussion threads. Once the contents have been shared on the forums, they become public goods resources that allow other users free access without restriction.

AutoHome has a reward system that functions as a club goods resource. To motivate users to participate in the forums' activities, AutoHome has implemented a membership hierarchy system of reward points that can increase membership level and be redeemed for small gifts (e.g., flashlight, gas card, and tire inflator) to encourage user participation. Since the rewards points can only be given to registered account users who are willing to create content, the reward points are club goods. However, membership level has no influence on digital services received and does not grant any privileges to users with higher membership levels. Users can earn some reward points which have some monetary value. Most participation is, however, voluntary and does not involve tangible returns, the monetary value of the reward points being negligible. For example, over a year and after being ranked as a top 10 contributor in a forum with over 20,000 registered users, I earned less than $50 worth of reward points that can be redeemed for gas cards or small gifts (e.g., tire inflator). Content providers are, in contrast, and according to my experiences and interaction with many content providers, motivated by the number of reads and replies and are therefore motivated by the amount of attention they can attract from other users.

In addition, to earn the participation reward, AutoHome users must register a user account. Registered users can earn membership rewards points by passive participation, such as visiting the forums they are interested in and logging into their account to check in or participating in OC activities, such as creating new threads, replying to others' threads, and answering others' questions. Passive participation can only earn small reward points, but the platform can issue a reward of up to 5,000 points to a high-quality content creator. Content providers are therefore motivated to earn high-quality content recognition from the platform to attract other users' attention. An awarded thread will be highlighted and can be filtered by other users. AutoHome encourages users to create high-quality content through two recognitions: Elite Content and Elite Homepage Content. Elite Content can be awarded by the informal forum moderator or the platform editor. The minimum requirements for elite content recognition are threads of at least 200 words and more than 15 photos. The Elite Homepage Content recognition is in addition to the Elite Content recognition and is only given to superior-high-quality threads that have the potential to attract thousands of reads and replies. An Elite Content recognition is not difficult to attain. All forums with no moderator that satisfies the minimum requirements will be automatically forwarded to the platform editor team. My observation and experience are that the platform editor team is very generous in awarding the Elite Content recognition and does not pay close attention to the actual content. Most forwarded threads with reasonable quality photos and of a reasonable length can attain this recognition. However, some car and insurance sales users take advantage of the Elite Content recognition process by reposting the same content to get other users' attention and promote their products.

It is, however, much more challenging to attain Elite Homepage Content recognition, partly due to the limited space of the homepage exhibit area; thus, Elite Homepage Content recognition seems

more like common-pool resources as it is non-exclusive, which all registered users could earn, but rivalrous, which is hard actually to get. Platform editors will only give this recognition to the pool of elite-content threads. Based on my observation, there is no fixed standard for Elite Homepage Content recognition. The recognition is, however, often awarded to threads about the user experience of a popular or exotic car, serial travel log, unique and high-quality content, or threads with a large number of reads and replies. Regular forum users also have to compete with professional editors who are hired by the platform or self-employed. Their threads are "automatically" granted Elite Homepage content recognition and can attract much greater attention. For example, my homepage thread only received 60,000 reads, which is very typical. Most of the professionally generated content with this recognition receives 500,000 to a few million reads.

The discussion forum thread's available spaces are common-pool resources. When the AutoHome users join a specific topic-based discussion forum (e.g., Tesla Model 3 Forum and Toyota Camry Forum), they will have the digital share places (i.e., discussion pages) to create threads. There is no limit on how many threads an individual user can create daily. Given the limited time and attention each community user is able to spend (Shen et al., 2015), it is unlikely that a user will be able to process all new threads created on their interested forum(s) due to the information processing cost (Sahoo et al., 2018). Indeed, based on my interactions with the Model 3 forum content creators and community lurkers, most of them will only check the first few pages of threads daily or even weekly. For instance, one model 3 forum user commented that:

"*Not only chatbots, but our forums also have so many users, who hate Tesla, [create content] to mislead others purposefully. As real registered car owners, we are not in the mood to communicate here. After checking a few pages of threads, I can barely find anything that is*

useful and valuable information. Instead, there are tons of malicious posts and hate. The forum discussion environment is ruined." Model 3 forum users comment (March 4, 2021)

Similarly, another model 3 forum user complained that

" *You are right. I want to see real [Model 3] car owners' car use experience, but I can barely find anything on the first page." Model 3 forum users reply to the previous comment* (March 4, 2021)

Insufficient use of digital spaces by the individual will lead to a shortage of available digital for the whole community group. The digital spaces, as a community resource, cannot be used for different purposes simultaneously as it only allows one user to create a single thread at a time. When a new thread is created, the existing thread will be put one position down. Digital forum spaces are rivalrous resources as the content creators compete for the first few "high-value" thread pages, creating incentives for users to compete with the community's attention. Also, the digital forum spaces are non-excludable. All registered AutoHome users, regardless of their interested forums, can create threads. Thus, even though the forum users' comments have shown that a forum can afford an infinite number of new threads, the threads are meaningless and useless if the content creators cannot get deserved attention (e.g., clicks and replies) (Shen et al., 2015). When the community grows larger, the forums contain many redundant and low-quality threads that even make the common-pool resources (i.e., digital space) even more scarce, creating a tragedy of the commons-like situation. Indeed, high-quality content is the main resource that attracts and retains users, as one platform editor commented.

"I think one of the most important resources is the user-generated content, but it is worth noting that this content also includes other users' replies. An online community discussion forum is the

place for users to communicate and exchange ideas. Users are more willing to see the user-generated content that they cannot easily see otherwhere. To produce high-quality content, the forum must have a sufficient number of users, and it also needs to have a forum leader to facilitate the discussion environment. Thus, the discussion forum is more like a system that needs many individual components to function…….you need to have a good forum leader to manage the community, a group of key opinion leaders to produce high-quality content, and you need to have the platform editors to help encourage the key opinion leaders to produce good contents. The most important, high-quality content deserved attention. You must have audiences. It is like an ecosystem." Platform editor's comments on platform resources.

The above comment has once more that the Authohome platform function more like a whole system, and its sustainability does not rely on any single component of the system, such as key option leaders or user-generated content but reply on all the individual components to work as a system to retain its sustainability.

A common is usually self-regulated due to its high administration cost(Ostrom, 1990). Similarly, with such a large daily active user base, AutoHome mainly implements a self-governance but with a hybrid governance system, potentially creating a commons-like situation. First, all forums are managed by a cross-forums violation report system, a link at the bottom of every thread allowing potentially violating content to be reported. The forum users can also use the same system to report complaints or violations to their forum moderators. The violation reporting system is very efficient and usually gives feedback within hours. The systems will delete the content and/or temporally or permanently close the associated accounts for the violated content and its associated accounts. Also, the platform editors will temporarily serve as the forum editor before appointing a forum

moderator. The same editor may several as the temporal forum moderator across multiple discussion forums until the forums have selected their moderators from the users.

Based on my observation, the temporal forum moderators, who are usually the platform editor team, play very limited roles in managing the forums' activities, and their responsibilities mainly focus on managing violated contents. In comparison, most forums are self-regulated by their appointed (a) forum moderator(s). Any user can voluntarily apply for the moderator position. However, there are many fixed requirements for becoming a moderator. First, users must be verified car owners of the forum. Second, users need to create at least three high-quality discussion threads. Third, users should not work for that company in the areas of automobile social media or the automobile industry. Users are therefore required to upload proof of employment and their official identity cards to verify this. The platform editor teams will act as acting moderators for forums without a moderator. They, however, mainly focus on promoting/selecting high-quality content instead of managing the forum's daily activities. In addition, the general responsibilities of forum moderators include highlighting/top the threads, appraisal of elite content, managing forum activities (e.g., deleting violating threads and resolving conflicts), organizing offline activities for forum users, and recommending high-quality threads to the platform editor for the homepage. The most distinct privilege for forum moderators is that they can share the third-party QR code to create the discussion group. The platform will automatically delete all shared QR codes, discussion group invitation links, and any other third-party messenger's ID that the moderators did not share.

4.4.2 Online community as a digital commons

An open-resource system needs to allow its stakeholder to continuously derive value to retain sustainability(Butler, 2001; Mindel et al., 2018), and the same principle applies to the digital commons. In my case, the digital common is the AutoHome platform.

Throughout my investigation, the Autohome platform is, for two reasons, a special form of commons which is a digital common property that sustains multiple types of resources to produce final services to its stakeholders. First, platform producers generally own the digital infrastructure. The digital infrastructure must, however, have some degree of public function that allows its stakeholders to derive value benefits from others. Content providers can derive value only when the content is "*consumed"* by others; content appropriators can derive value only when their effort is well-spent on the needed content; platform producers can derive value only when content appropriators and providers interact through their digital platforms. Second, the digital platform could be private property. However, it is costly for platform producers and individual users to exclude others (Faraj et al., 2015). For example, the US Supreme Court pending petition 593 suggests the exclusion of digital platforms such as Twitter and Facebook from the pure public forum, which is the "*property that the State has opened for expressive activity by part or all of the public. (1999)."* It also suggests that the law should restrict a platform's right to exclude, particularly where the platform becomes a public accommodation, and that the platform should be bound to serve all customers without discrimination. Therefore, the AutoHome open resource systems can be viewed as digital common property, the closest analog perhaps being an open-access marketplace where every stakeholder derives value through exchanging what they can offer for what they want. The best long-term interests of all are served by the marketplace's rules-in-use being fair, and goods being diverse and useful. A platform editor commented this view and replied to the following.

"Discussion forums are the open space for users to communicate and exchange new information. Users are willing to read the articles or threads they cannot easily find elsewhere. [Of course], the platform's most valuable resource is the users. However, it needs a dedicated forum leader to facilitate its users to create high-quality content. Also, discussion forms are part of and critical for the platform ecosystem. A high-quality article or thread may help the author to achieve great achievement. However, to retain the platform sustainability, the platform needs multiple moving components, and the discussion forum is key for the system sustainability. We need platform editors to retain users' engagement. Also, our discussion forum, especially the user-generated content, needs sufficient exposure to survive." Platform editor, interview

While the editor's comment shows that the discussion forum is an open and free space for users to interact, such an open-access platform could also create a common's situation for four reasons. First, although online community stakeholders could share common interests, it does not change the fact that people are self-interest and rational individuals who prioritize their own benefits over the group, creating the condition for collection action problems to emerge (Olson, 1971). For instance, a large amount of redundant and low-quality content was found during the investigation. Faraj et al. (2011) theorize the unique characteristic of online communities is fluidity which reflects the online community's boundaries, norms, participation artifacts, interactions, and foci continuously change over time. While fluidity makes digital interaction possible on an unparalleled scale and speed, the system offers "too much" freedom that collective action threats can emerge from individual-level actions (Mindel et al., 2018). Thus, like the conventional commons when attending to achieving individual and collective welfare, online communities are subject to inherent tensions between the community's interests as a group and the pursuit of individual gain, which dynamically affect its sustainability (Faraj et al., 2011; Mindel et al., 2018).

Second, an open digital resource system could suffer a free-riding problem because it shares similar system attributes as conventional commons. The recent theory developed by Mindel et al. (2018) conceptualizes OC as a type of information commons that shares three system characteristics with the conventional commons: low exclusion, high accessibility, and a high degree of freedom. First, the OC's sustainability relies on users' voluntary participation (Faraj et al., 2016; Mindel et al., 2018). While AutoHome offers the services for their interested users at no cost, similar to conventional physical commons, the low exclusion also creates a similar commons situation that the typical AutoHome users cannot exclude and be excluded by others, creating an incentive for individuals to act in the way that maximizes their own benefits while putting a little attention to community interests. Indeed, excluding users' participation usually requires collective decisions or decisions from the group representatives (Faraj et al., 2016). For instance, AutoHome always prefers to appoint an informal leader to manage the conflicts between users and avoid the ever-present danger of forking and balkanization(Fleming & Waguespack, 2007). An AutoHome editor comments on this:

"We mainly ask the forum moderators to manage their community……. We started to appoint forum moderators somewhere around 2007… they have many administration rights, such as deleting content and banning users' accounts. ……. the general guideline is that, as long as their administration does not hurt the users, we give them [moderators] a high degree of free down." Mr. Wu, platform manager interview

Third, the development of internet technologies makes the OCs highly accessible, where anyone can use the system without temporal and spatial constraints. The information exchange in the physical world usually requires people present at the same place and time. In contrast, digital-enabled communication allows both synchronous and asynchronous communication (Dennis et al.,

2008). Depending on the types of media use, IT affords different degrees of transmission and process capabilities (Dennis et al., 2008), such as the message can be sent and received simultaneously by many people, or a message can be retrieved and processed later on. While increasing the OC accessibility and membership size, Butler 2001 finds that community membership size has both positive and negative effects on OC sustainability. Specifically, the findings suggest that that the community with a large membership size tends to attract new users but brings challenges for retaining the existing users. Similarly, Bin et al. (2007) find that a community with a large number of activities may increase individual member participation cost. An individual with a higher information processing cost would prefer a smaller community size.

Last, while the OCs are a voluntary-based resource system, it inevitably causes the system to offer a high degree of freedom for its users to engage and interact with others and the technologies (Mindel et al., 2018), making the commons stakeholder free to disengage with little or no consideration of others. For instance, I have found a large number of forum users withdraw their participation from the AutoHome, and some of them even "delete" the community resources they created before when withdrawing. The decentralized information system makes it harder for the platform owner to enforce effective centralized governance, as OC users' behaviors are heavily self-regulated, as I discussed before.

4.4.3 From riding to free riding

The OC literature seems to define free-riding based solely on whether community users supply digital content forwards to others, which can be appropriated after benefiting the system. The selected typical free-riding behavior includes using but not contributing to open-source software (Baldwin & Clark, 2006), reading but not creating user-generated content (Wasko et al., 2004), and downloading but not sharing files on a P2P network (Adar & Huberman, 2000). It has therefore

been long thought that community lurkers, who only use the resource without providing it, free-ride the system because they do not contribute. For example, Mindel et al. (2018) define free-riding as "the extent to which appropriators evade information provision (p10)." But this is not always the case because riding for OCs can be an act that can be a contribution, and one cannot free ride without riding. One platform editor comments on his view on community lurkers' free-riding behavior.

"The purpose of the discussion forums is to give all interested users a place to communicate freely. Some people prefer to express and share their opinions and experiences, while others prefer to read the content to get the needed information. The discussion forum is such a place that allows users to get whatever they need freely. Thus, [reading but never creating content] is never a waste of resource for the platform." Platform editor, comments on community lurker.

His comment shows that it is not true that appropriating digital resources without provision is free riding. Community lurkers can indeed free-ride digital resources, but only if they have an obligation to contribute (Hess & Ostrom, 2007). Thus, my finding shows that whether the behavior is good or bad should be determined by the state of affairs they bring about (Driver, 2012; Mingers & Walsham, 2010; Scheffler, 1982). Free riding should, therefore, not be defined by what the behavior is but by its associated outcomes. If user appropriation of the digital resource does not increase others' participation costs (i.e., content provision and appropriation costs), they should not be considered free riders. In other words, riding for free does not equal free riding. Under certain conditions, reading but not creating content on a forum can be a contribution, as one platform editor expressed her similar view as us on the community lurkers.

No, [they are not wasting resources]. When the content creators share their experiences, they want audiences. Whether the audiences wish to reply or not, it should not be determined by the

platform but by the audiences themselves." Platform editors, comments on community lurker."

Platform editors, comments on community lurker.

Similarly, another platform editor shared his opinions on community lurkers.

"Based on the platform's traffic point of view, most users rarely create content, and this is normal. Because creating content costs time and effort, and many believe they may not get deserved return [others' attention], it is not worth it. ….. the lurkers are not wasting the platform resources. After all, the discussion forums are open to all ……. Reading but not creating content is not a waste of resources. Instead, it helps the platform get more internet traffic."

Platform editor interview

However, another platform raised his concern about community lurkers.

"I think that [reading but not creating content] is normal user behavior. However, for the platform, we need to pay attention to this because it may give us a warning that we should have a self-reflection to figure out what causes this problem. Several factors may contribute to this problem. First, our platform is not good. It could be that our products are not user-friendly. The user may need to spend too much time creating content, so the user may lose their passion for creating content. Second, there might be something wrong with the contents. Our platform is not attractive, the content classification algorithm is not good, and the contents are not comprehensive. Thus, the users are hard to find interesting content [to reply]. Last, our community discussion environment is not good, and users have no intention and interests to share." Platform editor, interview

Their comments have shown us that interaction with digital technologies is, to a certain degree, could be interpreted as a contribution. It also led us to rethink the boundary between resource

provision and appropriation, as the boundary between those two is blurred. At least on AutoHome, any interaction with the platform will leave a trace behind, and digital content provision needs to occur before or simultaneously with content appropriation. In other words, OC providers cannot derive value benefits without first providing the digital infrastructure; content providers cannot derive value benefits without creating content, and content appropriators cannot derive value benefits without devoting time and attention. In addition, the platform rarely views community lurkers are the burden of the platform. Instead, those lurkers could benefit the platform as a whole.

AutoHome's online community is open to all interested users. Meanwhile, all users have the right to express their opinions that might not be consistent with the forum's majority because it is a commons. One of the most interesting observations in the second resolution cycle was other regular users' interactions with forum distractors. These detractors are similar to internet trolls and intentionally upset people on the forums. The difference, however, is that their posts are not off-topic. They kept sharing negative, questionable information and news about Tesla and the Model 3, replying to almost every new forum user's question to persuade them to purchase something else. I thought, at the very beginning, that these detractors were hired by Tesla's competitor(s). However, after hundreds of interactions with them, I realized that some of them might be paid participants, but many are just regular users who want to get attention by expressing different opinions. One detractor replied to me:

"*I am an electrician, not an employee of XXX…. I just don't like Tesla, especially its CEO [Elon Musk] and his fans. I mean, Tesla does not have its own technologies. It did nothing but just assemble those outsourced parts together. The engine is from Taiwan, and the battery is from Japan…. Then they claim that it is the best electric car ever… what a joke! Tesla fans are*

brainwashed and brainless…I am here to help" *Interaction, multiple replies from a Model 3 forum distractor*

I spent hours with this distractor, trying to convince him that what he said was not true. However, it did not work. What I said had no impact on what he believed. This distractor remained very active until almost the end of this phase of the investigation and was ironically ranked the top contributor in the Model 3 forum for consecutive months but with no elite-content threads. Many regular forum users found his threads mostly entertaining but useful because he would always be the first person to share any negative news about Tesla. His account was temporally suspended many times. When his account was suspended, he used another account or registered a new one. Other long-term forum users quickly, however, recognized his new account by his unique writing style. This example has once again shown that the common interests do not warrant that the community users act in a way that benefits the community as a whole.

Many users, however, also think that these distractors are annoying and interrupting. Platform administrators did not, however, take any effective action, even though many Model 3 forum users reported the distractors' violations and asked platform administrators to suspend their accounts and IP addresses permanently. One long-term user wrote:

"*This is supposed to be a place for Tesla owners and enthusiasts to communicate. However, it is now occupied by tons of malicious detractors. I want to know, does AutoHome really care about managing this place? If not, there is no way we can keep using this place." (Observation, original thread in Model 3 forum)*

These distractors are more experienced than most forum users in the AutoHome participation policies, many being very active in multiple forums. I frequently found that their distracting

threads and replies were slightly below the threshold for sanctions (e.g., deleted content or account suspension). However, when community users tried to "*fight*" back, they were reported by the detractors and sanctioned. One user complained that:

"I think I now understand why those malicious distractors could keep annoying Tesla owners, spreading false information, and defaming Tesla and its fans. This forum indulges those distractors in abusing regular users but does not allow us to do the same. It was a joke that the forum administrator deleted my posts because they believed I was abusing the distractors. That explains why this forum communication environment is so bad. I know that Tesla does not have PR. AutoHome needs internet traffics and attracts users, and serves its VIP customers. I believe AutoHome is happy to see us fight with each other (distractors). The game is not fun when the judge is unfair." (Interaction, reply from a Model 3 forum user)

This observation aligns with the literature in that most open digital platforms offer almost non-exclusive services to users at no cost (Faraj et al., 2011; Mindel et al., 2018), but also create a commons situation in which typical OC users cannot exclude and be excluded by others, as excluding users' participation usually requires collective decisions or decisions of group representatives (Faraj et al., 2016). In addition to that, the platform's value benefits mainly depend on the internet traffic could generate by the forum's users. Regardless of the content they share, active users will eventually increase the value benefits for the platform owners. From the platform owner's perspective, they have less incentive to ban those "active" accounts. To validate my thought, I sought answers from other platform editors. One editor replied to her my thought on platform flaming debate:

"For the platform, it (flaming debates) indirectly proves that our forum is more active than others. The more flaming debate, the better for us to attract more attention. Just let them fight.

As long as the fight is not name-calling, we are happy to see them quarrel more with each other. "Interview, platform editor

This reply directed my attention to a plausible intentional ignorance of the platform that increases the participation cost for individual users. It is not surprising that the platform produces a motivation to tolerate a certain degree of "*flaming"* debates, as this helps the platform attract advertisers. When I asked the opinions of rival platform editors on platform tolerance of flaming debates, one replied:

"There are reasons for distractors, paid reviewers, and keyboard drivers. When your forum becomes large and popular, they are unavoidable. It indicates your forum is successful because the automobile manufacturers are willing to hire someone to manipulate customers' opinions. Those contents created by those guys are a double edge sword. When you manage it well, those flaming debates motivate more users to join the discussions. However, these could be harmful to your forum's overall discussion environment, and those useless content could flood the forum. Overall, the goodness or badness of distractor, paid reviewers, and keyboard drivers solely depend on the participation policies created and implemented by your forum moderators and platform editors." email interview, platform editor

Many editors raised similar concerns about managing forum activities when forums grow larger and become more popular. They, in particular, believe that it is difficult to distinguish suspected threads created by paid reviewers and distractors from the threads of regular users. They, therefore, hesitate to take any action. They also believe a certain level of flaming debates and advertorial content is good for the platform. "*At least, the existence of advertorial content indicates that your forum has some value. A forum without advertorial content is simply worthless*," one editor comments.

When the common (i.e., my discussion forums) becomes more valuable, it only attracts human users but also AI chatbots. I observed that AI chatbots control many inactive user accounts and answer forum user questions. AI chatbot accounts are very annoying and cause a great deal of confusion, especially to first-time forum users. The chatbots target question threads and are always the first to answer forum user questions. Sometimes the answers are meaningless such as "*you should contact your service center for this issue*." AI chatbots, however, tend to be very effective in answering redundant and simple questions by reusing the answers from previous question threads. Several interviewees from the outside of AutoHome organization suspect that AutoHome controls many AI chatbots on their platform because these accounts are highly identifiable that no human can answer multiple questions across multiple forums within seconds, but they refuse or hesitate to take effective action. It is also technically feasible and easily doable for a platform such as AutoHome to identify and ban those AI chatbots.

"Our IT teach design an algorithm that helps us detect AI chatbots. Once we find any threads created by AI chatbots, we will delete that contents. Meanwhile, we will permanently terminate its associated account." AutoHome platform manager, comments on AI chatbots

However, my observation tells us a different story. I purposely selected a few obvious AI chatbots control accounts that created multiple threads across multiple forums every few seconds. When I reported the chatbot accounts to the platform administrators' team, the administrators ignored my complaints. I returned to interviewees selectively to verify my finding, and an outside expert who implements AI chatbots on his platform commented that:

"Users want to get their questions answered. AI chatbots can significantly lower many platforms' administration costs and are good for retention. Currently, a supervised AI chatbot can generate 2000 to 3000 replies which is five times more efficient than an average editor."

Indeed, AutoHome, including other similar automobile discussion forums based on online communities, is facing an emerging challenge from the new social media, such as WeChat and TikTok. Some remain confident that discussion forums can compete in such a race to attract and retain sustainability. For instance, another social media platform comments the following.

"I disagree [that discussion forums are dying]. The discussion forums were born in the early days of Internet development and met the direct social needs of different groups of people. With the development of communication technologies, the form of social interaction has changed. As a result, instant messaging has been becoming the trend. However, social needs between different groups of people remain the same. ……. the most valuable part of the discussion forum is knowledge accumulation. Other instant-messaged based social media are more convenient but cannot accumulate knowledge because users are hard to find the previous message, and users, who join the chat group cannot view the previously discussed topics." Mr. Guan, Platform editor

While many editors I interacted with expressed a pessimistic opinion and worried about the challenges from other social media. For instance, an editor told us his concern.

"Online community discussion forum could be considered one of the very first internet product…… many functions originated from discussion forums have been replaced by modern social media…. For instance, when the user needs to ask a question, they, in the past, would ask the question from the forum, then wait for answers from other forum users. In comparison, the same user, in those days, could simply send the question to their WeChat group or TikTok to get an immediate response. Thus, he/she may no longer be willing to use the forum due to the delayed response. Similarly, the forum key opinion leaders may no longer prefer to use the discussion forum because of the less attention they get. For the same effort, the key opinion leaders can get much larger attention if they use WeiBo or TikTok. In those days, those key

opinion leaders are seeking the platform with large potential internet traffic…… as for the regular users, they can use WeChat to get the same needed information as they used the discussion forum, but with a much faster response… thus, the use of the discussion forum becomes less useful. "Mr. San, platform editor, comment.

To sum up, my major breakdowns can be summarized as information, or digital contents, are not the sole resources for the online community to produce its final services. The OC can be understood as a commons because it uses multiple resources, including public goods (i.e., digital content and social media platforms), common-pool resources (i.e., community shared space), etc., to produce the final services for its stakeholders. In addition, the self-governance management structure could cause a commons situation to emerge because common interests do not guarantee a sustainable social structure. Collective action to achieve group benefit is unlikely to occur even where common interests exist without a selective incentive to motivate self-regulated behaviors (Olson, 1971). OC stakeholders join together because of common interests. They can, however, also use and leave the community at will without considering the benefits and costs to others or that this will negatively impact the community's capability to maintain a pool of resources that continuously support other community stakeholders in the deriving of value benefits (Butler, 2001; Mindel et al., 2018).

Therefore, a deeper and more inclusive understanding of free riding in digital worlds is necessary. Free riding should not be simply viewed as consuming digital content without creating one. Because the consumption of the digital content will not result in any resource outflow, and that means the use of the digital content will not cause any depletion of the digital resource. Also, the community stakeholders cannot establish exclusive ownership over the content they consume (i.e., read or create), which means using the digital resource will not prevent others from using it.

Suppose the digital content is the only resource unit of the digital commons. In that case, the commons will become more sustainable through increased consumption because of the network effects, leading to the comedy, instead of the tragedy, of the commons (Mindel et al., 2018; Rose, 1986). Therefore, free-riding should not only apply to the content consumer but to all community stakeholders; whenever their interactions with the AutoHome platform increase the cost of others, they are the potential candidates for free-riders.

4.4.4 Understanding digital commons through the service-dominant logic

While the interaction of digital social media and the conventional commons management literature may provide theoretical insight on digital resource management, it generates many breakdowns that require us to solve to achieve an ethnographic understanding(Agar, 1986a). To resolve the breakdown, I followed Kozinets (2002) interpretive construct approach using another theory to interpret the findings. In this study, my interpretive construct is service-dominant logic(Vargo & Akaka, 2009; Vargo & Lusch, 2004; Vargo et al., 2008).

Service-dominant logic offers a broader view of the resources. That is, "*resources are a function of human appraisal and thus are often dynamic and potentially limitless; resources are a function of how something is or can be used and not a function of things per se (Lusch & Nambisan, 2015, p. 159).*" Resources have been conventionally viewed as those tangibles good that individuals use for support specific purposes, including natural resources (e.g., minerals and lands) and man-made resources (e.g., steel and roads)(Constantin & Lusch, 1994). Resources can also be in intangible forms, such as information(Mindel et al., 2018) and knowledge(Faraj et al., 2011; Hess & Ostrom, 2007).

Under the service-dominant logic view, the resources units in the AutoHome are not limited to one form, such as digital content, but extend to any other kinds of resources, such as digital space (e.g., Wikipedia's namespace) and tangible resource, such IT infrastructure, or simply users' interactions on the platforms, that the OC stakeholders could leverage to derive value. Together, all those resources form a service ecosystem. My findings have shown that the studied online community is a common-service system that contains public goods (e.g., platform and shared content), private goods (e.g., users' attention), club goods (e.g., membership rewards), and common-pool resources (e.g., forum shared thread spaces) to produce final service. Jointly, those multiple types of resources are required for AutoHome to produce the final services to all its stakeholders.

What role would the digital content play in such a service common system? S-D logic makes a distinction between operand resources and operant resources. ***Operand resources*** are "*resources that an actor acts on to obtain support," "while* ***operant resources****"* are resources that *"act on other resources to produce effects" (Lusch & Nambisan, 2015, p. 159).* In other words, operand resources are what AutoHome stakeholders need to use to derive value benefits, and operant resources are something that contains immediate value benefits for them to enjoy. It is worth noting that operand and operant resources are relative terms and are different for different AutoHome stakeholders. For instance, the platform owners need to supply and use the operand resources, which is the platform infrastructure, to attract users to use their platform, then the internet traffic generated by the users' interactions are the operant resources that can be used for the platform owners to sell advertisement. The content creators need forums' digital space to share their knowledge. In this case, the digital spaces and their knowledge are the operand resources, and the attention they attract and recognition they build are the operant resources. The content consumers need to visit the platform and devote their attention and efforts to find needed knowledge, and the

attention they devote and the threads they read are the operand resources, and the needed knowledge is their operant resources.

In addition, S-D logic suggests that digital resources (e.g., content and digital infrastructure) are still a part of service exchange but serve as the transmitters of the value co-creation process instead of the source of the value. Therefore, my interpretation and finding suggest that the resources provided by the OC stakeholder are operand resources to themselves and provide support to other stakeholders and that the resources appropriated from other stakeholders are operant resources that allow them to produce value benefits

Service-dominant logic solves the divide between resource providers and resource consumers. Service-dominant logic offers an actor-to-actor network view of the resource systems' participants who work with other actors to co-create value through resource integration and service provision. In adaption to my study, I no longer view individual OC's stakeholders (i.e., content provider, platform owner, and content consumer) as isolated entities but are loosely coupled social and economic actors who share overarching institutional logic and co-create value through service exchange. Thus, content creators could be the potential resources consumers because the content they provide could be served as a form of resource integration as they are using the common digital places to share their ideas and experiences while building their social capital (McLure Wasko & Faraj, 2005) or catch other's attention(Shen et al., 2015). The content creators can also be viewed as resource providers when the content creation is viewed as a form of service provision because content creation is conventionally viewed as knowledge collaboration (Faraj et al., 2015), and the content being shared can be used by other members to learn or co-create new knowledge. As the content creator, content consumer, and platforms become the resource integrator, free-riders should, based on the logic discussed above, not be limited to content appropriators (OC lurkers)

but could extend to include content providers because *worthless* provision could increase others' participation costs and diminish the value of service exchange. For example, an article's title seems to be good but turns out when read to be clickbait; the open-source software seems to be useful but turns out to be buggy or non-functional after installation; the P2P file appears to be the one needed but turns out, after download, to be a wrong file with a correct name. Platform producers can also free-ride the system when they fail to maintain the fairness of the service exchange.

4.4.5 Understanding free-riding through the service-dominant logic

Service-dominant logic defines a service system as a relatively self-contained, self-adjusting system where its social and economic actors are mostly loosely coupled and share overarching institutional logic and mutual value creation through service exchange (Lusch & Nambisan, 2015; Vargo et al., 2008). The normative function of service systems is to connect people, technology, and information through value propositions. Service systems aim to facilitate participants to integrate resources and exchange services within and across systems to co-create value. While the largest service system can comprise the global economy, the smallest service system can comprise the individual and his/her interactions with others (Normann, 2001).

The fundamental function of the OC platform is to allow its stakeholders to interact with others to exchange information. People cannot exchange information with themselves. OC's stakeholders similarly cannot create value without the presence of other users. I would therefore interpret digital resource withdrawal as being a bidirectional ***service exchange*** to which OC stakeholders apply their specialized competencies (e.g., knowledge, skills, and digital infrastructure) for the benefit of another entity and the entity itself (Lusch & Nambisan, 2015; Vargo & Lusch, 2004). In other words, operand resource provision needs to occur before or at the same as the operant resource consumption. For the individual users, any interaction with the IT platform will leave traces behind,

serving the potential operand resources for other OC stakeholders. For instance, every single click in my observed forum for any threads will increase the number of reads for the thread, which will help the content creator attract additional users and build their recognition.

Under the service-dominant logic view, AutoHome home stakeholders, including content creators, content consumers, community lurkers, and platform owners, are participants of the AutoHome service commons and resource integrators. I no longer view individual OC's stakeholders (i.e., content provider, platform owner, and content consumer) as isolated entities but loosely couple social and economic actors who share overarching institutional logic and co-create value through service exchange at the AutoHome community. Under this view, free riders no longer only apply to the community lurkers but all the participants when their participation is self-beneficial and harms the community interest.

Service-dominant logic has reconceptualized the value of the resources from value-in-exchange to. Value-in-exchange view indicates that value is embedded in the goods and is nominal. In comparison, value-in-context suggests that value is defined based on its ability to influence the exchange of resources, and the subsequence value could be derived by the resource exchange's participants. Here, under the service-dominant logic, value is phenomenological that the beneficiary uniquely and phenomenologically determines the value; value must be co-created that value is not created through isolated efforts of any resource exchange participants but through a combined action and process; value is multidimensional that value is coordinated through actor-generated institutions and institutional arrangements, in other words, the social and cultural context of the value determines what value is and how it is created; value is emergent that value comes into existence through relationships between an actor and the system.

Ostrom (1990) suggests that, for any open-resource system, "*it is essential to distinguish between the resource system and the flow of resource units produced by the system. (p30)"* to understand the processes of organizing and governing the commons. The resource unit is what individuals use from the system. Under the service-dominant logic, the resource unit is the service in which individuals apply their specialized competencies for the benefit of another entity and the entity itself (Lusch & Nambisan, 2015; Vargo & Lusch, 2004). Resource unit appropriation and provision determine the resource flow, which in turn influences the system's resource renewability. The system is renewable and sustainable where resource units are continuously withdrawn from the system in the range of the economic level of withdrawal. Even though the use of digital services, in general, could not cause any depletion. Based on service-dominant logic, the value of OC resources is no longer embedded within the resource. Still, it needs to be co-created through service exchange, stakeholders of the OC being the actors in a system of other actors, co-creating value through resource integration and service provision (Lusch & Nambisan, 2015). The digital resources and IT infrastructure could not be depleted. Still, the value of the service afforded by the IT infrastructure could be depleted because the value is not created until the beneficiary of the service, including all AutoHome stakeholders, integrates and applies those resources to produce the effect (Vargo & Akaka, 2009). Thus, even if the AutoHome stakeholders cannot physically withdraw resources, the *value of the resource could still be depleted* during the exchange process by stakeholder behaviors (i.e., service provision and resource integration) when their behaviors increase the cost of others' service exchange or break the fairness of the service exchange. For instance, when the system is flooded with a great deal of "*useless*" content, it causes sub-optimal outcomes for the *economic efficiency* of digital resource appropriation**.** This increases the cost of

appropriation or of digital resource provision**,** the system lacking appropriations that content provision is less beneficial and desirable.

To sum up, free riding indeed can exist in a free digital world. Free-riding could cause the value of the service exchange inside the digital common to be depleted, leading to the imbalance of service exchange when the resources outflow (i.e., service needed) is greater than the resource inflow (i.e., service provided.)

4.5 Discussion

Free-riding increasingly threatens open digital resource system sustainability and therefore is a problem that is important to manage. This is due to information technology (IT) diffusing into almost all aspects of human activity (Baskerville et al., 2020; Recker et al., 2021; Yoo, 2010). IT is no longer only being created to reflect reality but increasingly changing, meditating, or even creating reality (Baskerville et al., 2020; Recker et al., 2021). The increasing number of realities created or transformed into the digital world increases the tension between retaining a system's inclusivity, so making the digital world equally accessible, and the mitigation of the associated free-riding threats, free-riding giving any party the privilege to take advantage of others' efforts to sustain the system.

My study has demonstrated that it is necessary to re-evaluate the concept of free-riding. My ethnographic investigation has shown that free-riding should not be defined by what the behavior is but by its associated outcomes. When the community is supposed to be free and open to all to access, community lurkers may not be the free riders unless they have an obligation to contribute. In comparison, content creators and platform owners could free-riding the community when their supposed contribution, such as digital content created and IT infrastructure afforded, and

community rules implemented, hinder the service exchange that is needed by other community stakeholders.

Indeed, free-riding problems can originate from the provision or appropriation sides (Ostrom et al., 1994). Appropriation means that system users withdraw/use resource units from the system, such as raising cattle on a common pasture or driving on the public road. At Autohome, community lurkers are less likely to increase the participation cost of others. However, my findings also show that when the community lacks specific policies or rules that motivate the community lurker to transform into content creators. Especially when the forums are smaller and need more content contributors, it may negatively impact the whole platform ecosystem's sustainability, causing the yield of resource units, which is *service* in our case, between provision and appropriation to be unbalanced.

The free-riding problem that originates from the appropriation, which is service provision in my study, is the assignment problem (Ostrom, 1990). The assignment problem occurs when the production yield of resource units on a common's property may not be spatially homogeneous. Homogeneous resource distribution/production causes the assignment problem, leading to inefficient use of commons' resources. For example, a fishing ground may have a hot spot that allows more fish to be caught there than in other areas. If all fishermen fish in the hot spot, it will soon become a cold spot, with a much lower production yield than where all fishermen make a hot spot fishing rotation agreement.

Content creators and consumers' strategies on service provision (i.e., resource appropriation) can also cause suboptimal outcomes in service exchange. In other words, unfair service exchange in the digital commons could potentially cause long-term irreparable damage to digital commons' productive capability, harming the commons' productivity on operand resources. As I discussed

before, the resources, including operand resources, are a relative term, and the value of the resource should be determined by the beneficiaries, including content creators and content consumers. Thus, the operand resources could be the shared digital spaces and available digital content, and assignment problems could emerge from either the content creators' or content consumers' sides. For instance, based on content creators' point of view, over-posting and unfair allocation of content contribution rewards can demotivate content creators from creating future content, harming the productivity of the common operand resources. In contrast, the supply-side provision problem emphasizes the contribution to content provision and system maintenance. The commons create behavioral incentives for the individual to free-ride others' efforts to sustain the resource supply and maintain the system, including the community lurkers refusing to pay their fair share to maintain digital content to have sufficient content to sustain its longevity.

It is worth noting that a commons situation is a situation in which the common suffers from degrees of free-riding. Ostrom points out, however, that many commons situations are not dilemmas or evolve into the tragedy of the commons. For example, commons users are less likely to pursue strategies that mitigate the threats of free-riding when resource unit provision is sufficiently greater than demand (Ostrom et al., 1994). Free-riding becomes a commons dilemma when commons users are aware that (1) free-riding could cause sub-optimal outcomes that are not desirable from the perspective of the group but fail to achieve (2) a plausible and feasible institutional alternative arrangement that could improve the commons' current situation (Ostrom et al., 1994). The second boundary condition, which is an institutionally feasible alternative, indicates that there must be *"at least one set of coordinate strategies that are more efficient than current decisions and are institutionally feasible"* (Ostrom et al., 1994, p. 16). In other words, *Pareto Improvement* makes it possible for a proposed new institutional arrangement to help the commons achieve or get closer

to *Pareto Optimality*. Commons' stakeholders should, to achieve *Pareto Improvement*, coordinate strategies that increase the *economic efficiency* of resource allocation. Commons stakeholders also need to reach a sufficient level of consensus that changing existing institutional rules is necessary. However, for such a large social media platform as Autohome, reaching a sufficient level of consensus on changing existing institutional rules is extremely challenging. However, I should point out that AutoHome is not in the stage of a tragedy of the commons, but I have demonstrated how could free-riding could emerge from multiple types of AutoHome stakeholders. Also, we should keep in mind that while endeavoring to create equality that (through digital transformation) makes resources accessible at low cost, we may also be creating inequality for hard-working contributors whose efforts can be taken advantage of by free-riders.

4.6 Contributions and research implications

First, this study makes a significant contribution to OC literature by adapting and integrating common-pool resource literature with the service-dominant logic. One of the key challenges of adapting common-pool resource literature into the digital world is identifying the resource unit. Unlike the conventional physical commons, the resource system usually consists of one type of resource unit. This study has empirically illustrated that the digital commons' situation is more complex in the sense that the digital commons require multiple types of resource units to produce the final service to its stakeholders. Depending on the OC stakeholders' needs, they will be required to "withdraw" different types of resources to satisfy their heterogeneous needs. It is worth noting that digital resource appropriation and provision need to happen simultaneously as the only way to "withdraw" the resource is to interact with the digital commons first. Such interaction (e.g., content creation and consumption) will always leave traces behind that could serve as potential resources for other community members to consume. To understand this bidirectional resource

appropriation and provision, I adapt and extend the service-dominant logic to our study context. That being said, the digital resource provision and appropriation are viewed as a service-for-service exchange. During such a service exchange process, community stakeholders apply their competency (e.g., knowledge, attention, and IT infrastructure) to benefit others and reciprocally benefit themselves. This provides a fresh view of how the digital resource system could be depleted because even though some of the digital resources could not be depleted, its embedded value benefits, which the service recipient determines, could be diminished when unfair service-for-service exchange occurs.

For OC platform owners, one possible solution to avoid the digital commons' problem is increasing resource density according to the service-dominant logic. Here, ***density*** is the optimal allocation of resources at a particular time for a particular situation, and it is the process of "rebundling", "unbundling" and "liquefying" resources (Vargo & Akaka, 2009). Autohome could achieve this by increasing service provision that implementing the policies and rules to increase the density of operand resources that the platform afforded. Autohome could implement an effective tool that assists the content consumer to more easily decouple the needed information from the IT platform (Lusch & Nambisan, 2015) instead of manually searching or reading the whole forums. By doing this, the high-quality content can get more deserved attention, creating reciprocal input for content creators to co-create value through content provision. Indeed, service-dominant logic suggests that "*the goal of service systems is to provide input into the value-creating processes of other service systems and thus to obtain reciprocal input"* (Vargo & Akaka, 2009, p. 39).

In addition, the density of the service provision afforded by the OC platform should vary. Take the digital space afforded by the platform, for instance. Each digital space density could vary based

on the quality of the content it contains. The platform should allow its users, other than the content creator, to determine the content's quality to increase the digital space's density. For instance, AutoHome could implement similar “upvote” and “downvote” features that have already been successful on other discussion forum platforms (e.g., Reddit). When the content receives a sufficient number of upvotes, the content should be highlighted and/or last longer on the prime pages of the forum (e.g., the first page of the discussion forum).

In conclusion, sustaining the digital commons requires joint efforts from all OC stakeholders, including content consumers, content creators, and platform owners. We call for future studies to pay more attention to the possible free-riding behaviors arising from regular community users and the platform owners. We should pay closer attention to how OC stakeholders’ service-for-service exchange could potentially damage the long-term sustainability of the OC resources systems and what information technologies we should apply to create a fair service-for-service exchange. When the OC community size becomes larger, the free-riding behaviors are almost unavoidable, raising challenges for all OC stakeholders who want to create equality for all people enjoying the benefits of digitalization but also hesitate to make additional efforts to sustain the open resource system due to the burden of free-riders. This is a challenging area of research, and I hope my research findings can help encourage researchers further to extend the commons-pool resource literature and service-dominant logic to understand the digital commons’ sustainability issues.

References:

505 U. S. 672 678. (1999). International Society for Krishna Consciousness, Inc. v. Lee. *Supreme Court Cases: The Dynamic Court (1930-1999)*, N.PAG.

Adar, E., & Huberman, B. (2000). Free Riding on Gnutella. *First Monday*, *5*. https://doi.org/10.5210/fm.v5i10.792

Agar, M. (1986a). *Speaking of Ethnography*. Beverly Hills : Sage Publications, ©1986.

Agar, M. (1986b). *Speaking of Ethnography*. Sage.

Agar, M., & Hobbs, J. R. (1985). How to grow schemata out of interviews. In J. W. D. Dougherty (Ed.), *Directions in Cognitive Anthropology* (pp. 413-431). University of Illinois Press.

Anderies, J. M., & Janssen, M. A. (2016). *Sustaining the commons*. Arizona State University.

Baldwin, C. Y., & Clark, K. B. (2006). The Architecture of Participation: Does Code Architecture Mitigate Free Riding in the Open Source Development Model? *Management Science*, *52*(7), 1116-1127. https://doi.org/10.1287/mnsc.1060.0546

Baskerville, R. L., Myers, M. D., & Youngjin, Y. (2020). Digital First: The Ontological Reversal And New Challenges For Information Systems Research [Article]. *MIS Quarterly*, *44*(2), 509-523. https://doi.org/10.25300/MISQ/2020/14418

Butler, B. S. (2001). Membership Size, Communication Activity, and Sustainability: A Resource-Based Model of Online Social Structures [Article]. *Information Systems Research*, *12*(4), 346.

Constantin, J. A., & Lusch, R. F. (1994). *Understanding resource management : how todeploy your people, products and processes for maximum productivity*. The Planning Forum.

Dennis, A. R., Fuller, R. M., & Valacich, J. S. (2008). Media, Tasks, and Communication Processes: A Theory of Media Synchronicity. *MIS Quarterly*, *32*(3), 575-600. https://doi.org/10.2307/25148857

Driver, J. (2012). *Consequentialism*. Routledge.

Faraj, S., Jarvenpaa, S. L., & Majchrzak, A. (2011). Knowledge Collaboration in Online Communities [research-article]. *Organization Science*(5), 1224. https://doi.org/10.1287/orsc.1100.0614

Faraj, S., Kudaravalli, S., & Wasko, M. (2015). Leading Collaboration In Online Communities [Article]. *MIS Quarterly*, *39*(2), 393-412.

Faraj, S., von Krogh, G., Monteiro, E., & Lakhani, K. R. (2016). Online Community as Space for Knowledge Flows [Article]. *Information Systems Research*, *27*(4), 668-684. https://doi.org/10.1287/isre.2016.0682

Fleming, L., & Waguespack, D. M. (2007). Brokerage, Boundary Spanning, and Leadership in Open Innovation Communities [research-article]. *Organization Science*(2), 165. https://doi.org/10.1287/orsc.1060.0242

Forte, A., Larco, V., & Bruckman, A. (2009). Decentralization in Wikipedia Governance. *Journal of Management Information Systems*, *26*(1), 49-72.

Godwin, R. K., & Shepard, W. B. (1979). Forcing Squares, Triangles and Ellipses Into a Circular Paradigm: the Use of the Commons Dilemma in Examining the Allocation of Common Resources. *Western Political Quarterly*, *32*(3), 265-277. https://doi.org/10.1177/106591297903200304

Gordon, H. S. (1954). The Economic Theory of a Common-Property Resource: The Fishery [research-article]. *Journal of Political Economy*, *62*(2), 124-142.

Hardin, G. (1968). The Tragedy of the Commons [research-article]. *Science*(3859), 1243.
Hellmann, D., Maitland, C., & Tapia, A. (2016). Collaborative Analytics and Brokering in Digital Humanitarian Response. ACM Conference on Computer-Supported Cooperative Work and Social Computing, New York.
Hess, C., & Ostrom, E. (2003). Ideas, Artifacts, and Facilities: Information as a Common-Pool Resource [research-article]. *Law and Contemporary Problems*, *66*(1/2), 111-145.
Hess, C., & Ostrom, E. (2007). *Understanding Knowledge As a Commons : From Theory to Practice* [Book]. The MIT Press.
Hsu, Y.-C., Tsai, S.-L., Hsieh, M.-H., Jenks, M. S., Tsai, C.-H., & Hsu, M.-T. (2017). On My Own: A Qualitative Phenomenological Study of Mothers of Young Children with Autism Spectrum Disorder in Taiwan. *Journal of Applied Research in Intellectual Disabilities*, *30*(1), 147-156. https://doi.org/10.1111/jar.12229
Jaffe-Walter, R. (2020). Into the breakdown: embracing ethnographic confusion in challenging nationalist policy "truths". *International Journal of Qualitative Studies in Education*, *33*(2), 166-173. https://doi.org/10.1080/09518398.2019.1681547
Klein, H. K., & Myers, M. D. (1999). A Set of Principles For Conducting And Evaluating Interpretive Field Studies In Information Systems [Article]. *MIS Quarterly*, *23*(1), 67-93.
Kovarsky, D. (2016). A Retrospective Look at the Ethnography of Communication Disorders. *Journal of Interactional Research in Communication Disorders*, *7*(1), 1-25. https://doi.org/http://dx.doi.org/10.1558/jircd.v7i1.27511
Kozinets, R. V. (2002). The Field Behind the Screen: Using Netnography for Marketing Research in Online Communities [Article]. *Journal of Marketing Research (JMR)*, *39*(1), 61-72.
Kozinets, R. V. (2010). *Netnography : doing ethnographic research online*. SAGE.

Le Trividic Harrache, L. (2017). How did I become an abductive ethnographer? Reflections on a research journey. *Journal of Organizational Ethnography*, *6*(2), 129-143. https://doi.org/10.1108/JOE-03-2017-0017
Lusch, R. F., & Nambisan, S. (2015). Service Innovation: A Service-Dominant Logic Perspective [Article]. *MIS Quarterly*, *39*(1), 155-176.
McLure Wasko, M., & Faraj, S. (2005). Why Should I Share? Examining Social Capital And Knowledge Contribution In Electronic Networks Of Practice [Article]. *MIS Quarterly*, *29*(1), 35-57. https://doi.org/10.2307/25148667
Mindel, V., Mathiassen, L., & Rai, A. (2018). The Sustainability Of Polycentric Information Commons [Article]. *MIS Quarterly*, *42*(2), 607-A614. https://doi.org/10.25300/MISQ/2018/14015
Mingers, J., & Walsham, G. (2010). Toward Ethical Information Systems: The Contribution of Discourse Ethics. *MIS Quarterly*, *34*(4), 833-854. https://doi.org/10.2307/25750707
Normann, R. (2001). *Reframing business : when the map changes the landscape*. Wiley.

O'Mahony, S., & Ferraro, F. (2007). The Emergence of Governance in an Open Source Community. *Academy of Management Journal*, *50*(5), 1079-1106. https://doi.org/10.5465/amj.2007.27169153
Olson, M. (1971). *The Logic of Collective Action: Public Goods and the Theory of Groups, Second Printing with a New Preface and Appendix*. Harvard University Press. https://doi.org/10.2307/j.ctvjsf3ts

Ostrom, E. (1965). *Public Entrepreneurship: A Case Study in Ground Water Basin Management* University of California-Los Angeles, Department of Political Science]. http://hdl.handle.net/10535/3581

Ostrom, E. (1990). *Governing the commons : the evolution of institutions for collective action*. Cambridge; New York : Cambridge University Press, 1990.

Ostrom, E. (2009). A General Framework for Analyzing Sustainability of Social-Ecological Systems [10.1126/science.1172133]. *Science*, *325*(5939), 419.

Ostrom, E., Gardner, R., & Walker, J. (1994). *Rules, games, and common-pool resources*. University of Michigan Press.

Recker, J., Lukyanenko, R., Jabbari, M., Samuel, B. M., & Castellanos, A. (2021). From Representation To Mediation: A New Agenda For Conceptual Modeling Research In A Digital World [Article]. *MIS Quarterly*, *45*(1), 269-300. https://doi.org/10.25300/MISQ/2021/16027

Rose, C. (1986). The Comedy of the Commons: Custom, Commerce, and Inherently Public Property [research-article]. *The University of Chicago Law Review*, *53*(3), 711-781. https://doi.org/10.2307/1599583

Sahoo, N., Dellarocas, C., & Srinivasan, S. (2018). The Impact of Online Product Reviews on Product Returns. *Information Systems Research*, *29*(3), 723-738. https://doi.org/10.1287/isre.2017.0736

Savas, E. S. (1977). Alternatives for delivering public services : toward improved performance. In *Westview special studies in public systems management*. Westview Press.

Scheffler, S. (1982). *The Rejection of Consequentialism : A Philosophical Investigation of the Considerations Underlying Rival Moral Conceptions* (Vol. Rev. ed) [Book]. OUP Premium.

Schultze, U. (2000). A Confessional Account of an Ethnography about Knowledge Work. *MIS Quarterly*, *24*(1), 3-41. https://doi.org/10.2307/3250978

Shen, W., Hu, Y. J., & Ulmer, J. R. (2015). Competing for attention: an empirical study of online reviewers' strategic behavior. *MIS Q.*, *39*(3), 683–696. https://doi.org/10.25300/misq/2015/39.3.08

Thompson, M. (2005). Structural and Epistemic Parameters in Communities of Practice [research-article]. *Organization Science*(2), 151. https://doi.org/10.1287/orsc.1050.0120

Tiwana, A. (2008). Governance-Knowledge Fit in Systems Development Projects. *Information Systems Research*, *20*(2), 180-197. https://doi.org/10.1287/isre.1070.0164

Van de Ven, A. H. (2007). *Engaged scholarship : a guide for organizational and social research*. Oxford ; New York : Oxford University Press, 2007.

van den Broek, E., Sergeeva, A., & Huysman, M. (2021). When The Machine Meets The Expert: An Ethnography Of Developing Ai For Hiring [Article]. *MIS Quarterly*, *45*(3), 1557-1580. https://doi.org/10.25300/MISQ/2021/16559

Vargo, S. L., & Akaka, M. A. (2009). Service-Dominant Logic as a Foundation for Service Science: Clarifications. *Service Science*, *1*(1), 32-41. https://doi.org/10.1287/serv.1.1.32

Vargo, S. L., & Lusch, R. F. (2004). Evolving to a New Dominant Logic for Marketing. *Journal of Marketing*, *68*(1), 1-17. https://doi.org/10.1509/jmkg.68.1.1.24036

Vargo, S. L., Maglio, P. P., & Akaka, M. A. (2008). On value and value co-creation: A service systems and service logic perspective. *European Management Journal*, *26*(3), 145-152. https://doi.org/https://doi.org/10.1016/j.emj.2008.04.003

Wang, P. (2018). *The emerging control tension around the user-generated content in the online community* International Conference on Information Systems, San Francisco. https://aisel.aisnet.org/icis2018/social/Presentations/9

Wang, P., & Baskerville, R. L. (2019). *User Self-Destruction: Theorizing Behavioral Transitions from Cognitive Absorption to Cognitive Discharge* Pacific Asia Conference on Information Systems, Xian, China. https://aisel.aisnet.org/pacis2019/182

Wasko, M. M., Faraj, S., & Teigland, R. (2004). Collective Action and Knowledge Contribution in Electronic Networks of Practice [Article]. *Journal of the Association for Information Systems*, *5*(11/12), 493-513.

Wettergren, Å., & Bergman Blix, S. (2016). Empathy and objectivity in the legal procedure: the case of Swedish prosecutors. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *17*(1), 19-35. https://doi.org/10.1080/14043858.2015.1136501

Yoo, Y. (2010). Computing in Everyday Life: A Call for Research on Experiential Computing. *MIS Quarterly*, *34*(2), 213-231. https://doi.org/10.2307/20721425

Chapter 4 Postscript

The existing online community literature defines free riding based solely on whether community users deliver digital content forward to others, which can be appropriated afterward and benefiting the system. It has therefore been long thought that community lurkers, who only use the resource without adding to it, free-ride the system. This study re-evaluated and challenged the original concept of free-riding by implementing a longitudinal ethnographic study. The study calls on other researchers to exercise caution on the notion that riding for free is not free riding. When the community becomes large and popular, the community will inevitably have a large number of community lurkers. Still, they are not free riders because their resource appropriation does not increase the participation cost of others. Instead, they are motivating more content contributors.

However, this study also shows the possibilities of technology-induced free-riding behavior when the community resources are widely accessible because of the development of new information technologies (e.g., mobile apps recently introduced by AutoHome). The community member may decide whether he or she should share the cost of sustaining the community (i.e., digital resources appropriation and provision). Indeed, individual community members are motivated to minimize the cost of resource appropriation and provision. This may negatively impact the digital resource systems sustainability because it is in the community's best interest to sustain the digital sources by fairly sharing the cost across all members. With the digital resources becoming more valuable when it is more accessible and being used by more members, the additional accessibility of the resource system could inspire more free-riding behaviors, causing the system to become less sustainable.

Chapter 5. Thesis Conclusions

5.1 Reprise - Objective

Motivated by the importance of digitalization, its associated unanticipated outcomes, and the need for a deeper understanding of the conflicting interests between individuals' rational decisions and rational outcomes at the system level, this dissertation set out to provide insights to address the following research questions: *can we explain how individual actions, resulting from individual rational decisions, respect, or fail to respect, the principle of rational decisions at the system (or collective) level?* In other words, w*hat are the negative impacts of individual rational decisions on information system sustainability?*

To answer these questions, I offered method triangulation (i.e., an ethnographic study, an experimental study, and a literature review study) through findings translations leading to indications for an overall conclusion. I examined the individual rational decisions on system use and technology artifact design and provided the findings against the assumption that individual rational decisions will always lead to better collective system outcomes. This dissertation highlighted three plausible unanticipated consequences of digitalization by demonstrating how IT can be designed, used, and interpreted by human agents beyond its original intent and produce a diminishing effect on the system's sustainability. My method triangulation response to the recent call for the researcher to leverage epistemologically and ontologically diverse information system disciplines to form agile responses to changes in contexts for IT development and use (Thatcher et al., 2018).

5.2 Contributions

In chapter 2, our research challenges this assumption by showing that the information system could be more vulnerable when security technologies cause system users to make more risky decisions. Thus, our study investigates the paradoxical relationship between security investment (i.e., adopting security technologies) and system risks (i.e., system users' risk-taking behavior) at the individual level. We posit that system user risk-taking behaviors could significantly diminish technological protection benefits.

Conventional wisdom believes that information security technologies can help us improve system security. My research findings have challenged this assumption by presenting the evidence that the information systems could be more vulnerable when security technologies cause system users to make more risky decisions. My study investigated the paradoxical relationship between security investment (i.e., adopting security technologies) and system risks (i.e., system users' risk-taking behavior) at the individual level. This makes practical contributions by explaining why and how security technology investment could lead to insecure behaviors and plausibly cause more risk exposure that puts organization information systems in danger. It is, however, worth noting that our findings should provide new, non-exhaustive, and exclusive causal explanations. It is correct to say that we have examined this paradoxical relationship at the individual level. This should not, however, diminish our contributions. Individual users are primarily a part of the information system. It is, therefore, necessary to know under what conditions our weakest node would become even more vulnerable. To sum up, this study highlights that system user risk-taking behaviors could significantly diminish technological protection benefits.

In chapter 3, I conducted a literature review to zoom into cybersecurity literature to see how cybersecurity scholars see the effectiveness of two-factor authentication technology in reducing

cybersecurity risks. After analyzing 55 two-factor authentication studies from ABI/Inform and EBSCOhost, I challenge the assumption that strong evidence supports the argument that two-factor authentication can provide better security protection. I find that the research pattern of the two-factor authentication discipline has fallen into an undesirable "break-fix-break-fix" cycle. I also find strong evidence that many new proposed two-factor authentication schema can bring many unexpected risks. I summarized those unexpected risks into three themes, namely, problem-centered weakness, solution-centered weakness, and user-centered weakness, to provide guidance for future cybersecurity research.

In chapter 4, the communication technologies are designed to help human agents to create an inclusive and free digital world. However, this essay demonstrates that the technologies create the conditions in which free-riding problems can arise. This study challenges the conventional understanding that content consumers who only read but never create new content are free riders by synthesizing how different online community stakeholders view those supposed "free-riders." This study posits that free-riding should not be determined by what behavior is but by its associated outcomes. When consuming the content does not increase the participation cost of others, the content consumers are not free-riding. Instead, free-riding arises from the content creators and platform owners when one content creator creates work for another. That is a free ride. This study calls our attention to the issue when we endeavor to create equality that, through digitalization, makes resources accessible at low cost. It may also generate inequality for hard-working contributors whose efforts can be taken advantage of by free riders.

5.3 Responses to Thesis Research Theme

How do we ensure individual actions resulting from individual rational decisions respect the principle of rational decisions at the system (or collective) level? Again, I should acknowledge that this thesis does not intend to find a universal solution to fit all information sustainability issues. Rather, this thesis aims to provide insights for future research on how individual decisions in IT use contexts may introduce system weakness and failure points.

Table 5-1. Thesis Individual Themes Summary

	Social collective's ideal outcome	Individual Decision Point	Individual self-interest Ideal Outcome	System Failure Point
Chapter 2	Increased security system reliability	Whether or not to relax security-related behaviors when security technology is beefed	More focus on expected utility maximization of chosen actions	Additional security technology is defeated by inspiring more relaxed security behaviors
Chapter 3	Decrease authentication factors embedded risks	Whether or not to introduce a second authentication factor when needed to mitigate the embedded risks in the simple-and-poor passwords.	More focus on retaining system convenience when increasing system security	Additional two-factor authentication artifacts are defeated by more vulnerabilities in the chosen second authentication factor
Chapter 4	Increased digital resource system sustainability	Whether or not to share the cost of sustaining the community when community resources are accessible.	More focus on minimizing the cost of resource appropriation and provision	Additional digital resources accessibility by inspiring more free-riders

Chapter 2 Responses

Specifically, in chapter 2, the individual decision point is whether or not the individual system users should relax their security behaviors (i.e., choose less secure but more convenient decisions when the information security technology is present). In this scenario, the study demonstrates that individuals are motivated to maximize the expected utility of the chosen decision according to their system environment change, causing the system failure point that the inspired risk-taking

behavior diminishes additional security technology protection benefits. Collectively, if more users make more risky security decisions, the information security system will become less reliable and could be defeated by future threat events.

Chapter 3 Responses

In chapter 3, the individual decision point is whether or not to introduce a second authentication factor when we need additional security technology to mitigate the risks embedded in the users' chosen simple-and-poor passwords. The general assumption when designing new technology artifacts is that the technology designers need to balance the costs and benefits of implementing new security technology (i.e., two-factor authentication in my study) because the users are motivated to retain the same level or more convenience when they need to use new security technology to protect their or organizational assets. However, my literature view demonstrates that the introduced second-factor authentication could be embedded with more security risks, which could diminish the protection benefits of introducing additional authentication factors, causing system failure points.

Chapter 4 Responses

In chapter 4, the individual decision point is whether or not the individual online community members should share the cost of sustaining the community (i.e., digital resources appropriation and provision) when community resources are widely accessible. The study demonstrates the tensions between individual community stakeholders, motivated to minimize the cost of resource appropriation and provision, and the community as a whole motivated to sustain the digital sources by fairly sharing the cost across all stakeholders. With the digital resources becoming more

valuable when it is more accessible and being used by more members, the additional accessibility of the resource system could inspire more free-riding behaviors.

Responses of the Three Essays Collectively

The findings from all three essays could translate into each other to yield overall findings that answer my thesis's research questions by using Orlikowski (1992) 's duality of technology to interpret my findings. The duality of technology offers us a solution to the dilemma of (1) choosing individual self-interest rational decisions and (2) collective interests of system outcomes and allows them to embrace both. Orlikowski (1992) suggests that technology is the result of human activity while simultaneously assuming the attributes of its afforded structure. Thus, whether the technology use is good or bad for system sustainability depends on the numerous meanings the human agent attached to it within a given social context. In other words, the good or bad of technology is influenced by how human agents design, implement and use the IT in its embedded social and organizational context. This dissertation shows that, while the personal action of human agents using technology has a direct on local conditions, it also has an indirect effect, either intended or unintended, on the system environment and the system sustainability in which the agents are situated. In other words, this thesis indicates that, while individual rational decisions influence and are constrained by information systems' abilities to allow users to derive value benefits continuously, their actions are the driving and diminishing force for the system's sustainability.

Balancing the tradeoff between individual autonomy and system outcomes is the key to answering my thesis research questions. In chapter 2, personal autonomy reflects the ability to exercise a degree of control over the purposes of IT use to achieve work performance (Mazmanian et al., 2013), while collective outcomes reflect the overall information system security risks. When we

over-advertise the protection benefits of information security technologies, my findings suggest that it may cause an unnecessary security decision tradeoff where individual insecurity action could potentially introduce more system vulnerabilities than the technology could mitigate. This tradeoff is especially true as our essay shows that non-functional security technology may not trigger additional user protection behavior. Thus, the unbalanced tradeoff between technology protection and individual risk-taking behavior could cause unanticipated consequences that diminish the value of information security technologies, causing information security systems to become less sustainable.

In chapter 3, personal autonomy reflects the cybersecurity researchers' self-evidencing belief in the effectiveness of two-factor authentication artifacts. Chapter 3 highlights the additional embedded risk with those newly designed technology artifacts. The discipline of two-factor authentication seems to fall into the undesirable "break-fix-break-fix" cycle, hindering the development of the two-factor authentication as a whole paradigm. This essay calls for researchers' attention to use a consistent performance evaluation method for the effectiveness of two-factor authentication artifacts. I recommend future research in this area should rely on experiments or simulations to evaluate the performance of these authentication systems consistently. For instance, experiments and simulation methods use empirical data to generate consistent measurements, such as false rejection, acceptance rates, and system processing time. By doing this, we can better understand the embedded weaknesses and strengths in various combinations of different authentication technologies, promoting the development and implementation of two-factor authentication.

In chapter 4, personal autonomy is a reflection of social media use that "users of social media enjoy a high degree of flexibility to determine which social media to use, when and to what extent, what

to create, what to share, and what to read" (Karahanna et al., 2018, p. 739). In comparison, the collective outcomes reflect the creation of a sustainable open digital resources system. The unbalanced tradeoff between those two could cause the unintended consequences that individual efforts to sustain the collective systems could be free-ridden by others because of the systems' high degrees of freedom.

In conclusion, this dissertation presents three plausible anticipated outcomes of digitalization. It also empirically demonstrates how human agents, including regular IT users and researchers, can interpret the meaning of IT in ways that maximize their own interests but may collectively cause undesirable outcomes in the perspective of the systems. Although this dissertation focuses on the negative aspects of digitalization, I do not intend to go against digitalization. Instead, I aim to promote digitalization by identifying potential downsides during such a process and providing insights to other scholars to mitigate the risks of the digitalization process. This dissertation is the result of my Ph.D. journey at Georgia State University. Something important I learned from this dissertation is to use the correct research methodologies to answer the correct research question, avoiding type III errors as specified by Rai (2017). For instance, I planned to use text-mining for chapter 4 at the initial stage of the project. However, I soon discovered that the only way to understand the meaning behind those texts is through interpretation and emerging myself into the study context. Understanding the text without considering its context may cause misinterpretation. Last but not least, I would like to express my gratitude to all the faculty members at the Computer Information System Department of Georgia State University. Without your guys' great help and training, this dissertation is not going to be possible. Thank you.

References:

Karahanna, E., Xu, S. X., Xu, Y., & Zhang, N. A. (2018). The needs–affordances–features perspective for the use of social media. *MIS Q.*, *42*(3), 737–756. https://doi.org/10.25300/misq/2018/11492

Mazmanian, M., Orlikowski, W. J., & Yates, J. (2013). The Autonomy Paradox: The Implications of Mobile Email Devices for Knowledge Professionals. *Organization Science*, *24*(5), 1337-1357. https://doi.org/10.1287/orsc.1120.0806

Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, *3*(3), 398-427. https://doi.org/10.1287/orsc.3.3.398

Rai, A. (2017). Avoiding Type III Errors: Formulating IS Research Problems that Matter [Article]. *MIS Quarterly*, *41*(2), iii-vii.

Thatcher, J., Pu, W., & Pienta, D. (2018). IS Information Systems a (Social) Science? *Communications of the Association for Information Systems*, *43*(1), 11.