MOTOR IMPULSIVITY AND INDIVIDUAL BEHAVIOR IN CLOUD BUSINESS: PRIVACY AS A MEDIATOR AND OPENNESS AS A PERSONALITY TRAIT SHAPING SECURITY DYNAMICS

Karuna Kothapalli

A Dissertation

Submitted to Franklin University in partial fulfillment of
the requirements for the degree of

DOCTORATE OF BUSINESS ADMINISTRATION

November, 2025

Committee:

Dr.Timothy Reymann, Committee Chair

Dr. Lori Salgado, Committee Member

Dr. Lewis Chongwony, Committee Member

Franklin University

This is to certify that the dissertation prepared by

Karuna Kothapalli

"Motor Impulsivity and Individual Behavior in Cloud Business: Privacy as a Mediator and Openness as a Personality Trait Shaping Security Dynamics"

Has been approved by the committee as satisfactory completion of the dissertation requirements for the degree of

Doctor of Business Administration

Tim Reymann (Nov 11, 2025 07:49:47 EST) — 11/11/2025

Dr. Tim Reymann, Committee Chair & Doctoral Adjunct
Franklin University

Lori Salgado (Nov 20, 2025 19:13:14 MST) — 11/20/2025

Dr. Lori Salgado, Committee Member & Doctoral Adjunct
Franklin University

Lewis Chongwony (Dec 1, 2025 00:41:42 EST) — 12/01/2025

Dr. Lewis Chongwony, Committee Member & Dir. of Research Core
Franklin University

Robin Hinkle (Dec 1, 2025 08:20:59 EST) — 12/01/2025

Dr. Robin Hinkle, DBA Program Chair
Franklin University

Wendell Seaborne, PhD (Dec 1, 2025 08:23:26 EST) — 12/01/2025

Dr. Wendell Seaborne, Dean, Doctoral Studies
Franklin University

FRANKLIN UNIVERSITY
Doctoral Studies

Note: This form is issued using the name listed on the student's official record.

(THIS PAGE WAS INTENTIONALLY LEFT BLANK)

Abstract

Literature has paid considerable attention to the study of impulsivity and personality characteristics on aspects such as risk-taking behavior and privacy concern in other contexts, but little light has been shed on how they combine among people in cloud business and data security setting. The current study filled a significant void by quantitatively examining how motor impulsivity was combined with openness to experience trait of personality and personal information privacy on one's behavior in the cloud business and data security environment. A total of 150 cloud business and technical professionals in financial companies were sampled. Risk propensity model was utilized as a framework. This study investigated two primary research questions regarding the relationship between motor impulsivity and individual behavior. Specifically, it examined whether personal information privacy mediated this relationship and whether openness to experience moderated the strength or direction of this effect. There were statistically significant results which led to the rejection of all three null hypotheses as stated in the research question. Suggestions ranged from a program to assessing impulsive behavior, tailored training modules, and personalized security measures. It would be interesting for future work to investigate the moderating effects of other personality traits on impulsivity and personal behavior, as well as to study how cultural dimensions shape security behavior.

Dedication

I praise Almighty God for His immeasurable blessings and guidance along my path. Your wisdom guidance and strength divine have brought me here, Protected, giving me the guts to meet and rise and dare. Thank You for Your constant LOVE, PROTECTION & GRACE, You light the way, and You fill my hearts with hope & THANK You THANK YOU THANK You!!!

I couldn't imagine the things I could do for myself when I made it to the U.S, and finally getting a doctorate was one of them. It is the end of my thesis and graduate life that I wish to dedicate this thesis to my wonderful family and to my loving parents, that have always believed in me and supported me in all my ways. My dear brother - You are a rock of unwavering support. To my dear daughter, who is constantly motivating me to be my best. And to my incredible husband, whose endless love and support has made this journey possible. And this was as much your accomplishment as it was mine. Thank you all for your constant love and support.

Acknowledgments

First and foremost, I would like to extend my huge admiration to my mentor and advisor, Dr. Timothy Reymann, for his unparalleled guidance during this research. I do not have words to express the steady leadership of Dr. Timothy Reymann's unwavering leadership or his consistent encouragement throughout the doctoral journey and process of conducting this study. I would like to thank him for taking time to settle my research and counseling me towards areas with weaknesses.

I am grateful to Dr Lewis Chongwony for his tremendous encouragement and advice on my research methodology. You've also provided an invaluable feedback on the development of the study and its rigor and validity. Thank you so much for your dedication and time helping me through some impressive methodology! Thanks for being part of this journey.

I want to acknowledge Dr. Lori Salgado's incredible support and knowledge throughout, particularly when she joined as an alternate and made a significant impact on committee review. It truly would not be possible for me to have done this research without your expertise and input and your dedication to the journey has made my experience better.

The Committee's timely and thorough feedback led to a much stronger project. Thank you for caring and for being so critical in upholding the quality and the substance of this work. You have been an inspiration, and I really appreciate the time and effort you have put in.

My thanks to Franklin University Technology and Library resources enabling my research as well as my degree.

Table of Contents

Page

List of Figures

List of Tables

Chapter 1: Introduction

A data breach is commonly defined as the loss of massive amounts of data. The impacts of security vulnerabilities and data breaches continue to rise, with human errors occurring at a higher rate (Brown, 2025). According to Pimenta Rodrigues et al. (2024), research on data breaches globally has revealed that organizations often fail to classify business and personal data, resulting in a loss of focus on human errors that can lead to unauthorized or accidental access, disclosure, alteration, loss, or destruction of personal information. This evidence emphasized the need to complement technical defenses with a focus on human-centric vulnerability to strengthen resilience among cloud businesses and in cybersecurity. However, there were not enough statistical studies to demonstrate the influence of personality traits on cloud security decision-making, which is what this study investigated. The global phenomenon of cloud business model approaches and the paradigm shift to adopt cloud networks has increased reliance on technology platforms, leading to unprecedented threats and vulnerabilities in digital information systems (Ahmadi, 2024).

A recent study highlighted that organizations often fail to detect insider threats and malicious employee behavior (Ding et al., 2024). According to current cybersecurity analyses, categorizing data flows and activities of business and technology users remains a widely accepted framework for understanding insider threats and unauthorized access (Suntwal et al., 2025). Furthermore, research indicated that even cybercriminals leveraged these classifications to construct fragmented identities, blurring the lines between hackers and professionals (Stackpole, 2024). In cybersecurity and human behavioral analysis, an intricate relationship existed between impulsivity domains, personal information privacy concerns, and Big Five personality traits (Khadka & Ullah, 2025). Several scholars have emphasized the integration of

behavioral insights into business continuity and security strategies, illustrating how impulsiveness and personality factors influence security decision-making (Akeiber, 2025; Almansoori et al., 2023). As Nifakos et al. (2024, pp. 173–184) emphasized, social engineering tactics were particularly effective within critical information infrastructures, where human factors remain a significant security concern as they exploit social engineering to exploit behavioral tendencies and perceived urgency to bypass technical security measures. International Business Machines Corporation (IBM) reported a significant increase in global data breaches in 2024, with the average post-breach costs reaching $4.8 million, a 10% rise from 2023. However, the national average cost of a single data breach within the United States in 2024 reached an all-time high, compounding to a 15% increase over the last three 3 years, equating to around $9.6 million in addition to the countless damages to the company's reputation and recovery costs (IBM, 2024). The IBM report also illustrated that an average recovery time of 280 days was required to identify customer data loss and effectively contain the data breach. According to Morgan (2020) says cybercrime costs will reach $10.5 trillion by 2025. However, Cadwell (2023) reported that a data breach typically costs $5.09 million in the United States, significantly more expensive than the average data breach costs in global regions.

Recent reports have indicated that data breaches persist despite enforcing the General Data Protection Regulation in Europe. According to de Souza (2025), the total fines under GDPR have reached €5.88 billion. However, the average cost of cloud data breaches was $3.8 million, and 45% of data breaches occurred in cloud environments (Cadwell, 2023). According to a Kaspersky press release, intentional employee actions violating organizational security protocols contributed to 33% of data breaches, which can be considered insider threats (Faro, 2023). Loss of customer trust, reputational damage, and legal sanctions had long-term effects on a company's

image and sustainability. Petrosyan (2025) reported that the most significant data breach incident was the Yahoo data breach between 2013 and 2016, which affected three billion online users worldwide due to security intrusions by malicious actors. Insider threats can damage a brand's reputation and lead to monetary losses, while security breaches caused by internal personnel can significantly erode trust and undermine credibility (Clifton, 2024). Verizon's (2025) 2025 Data Breach Investigations Report revealed that 57% of organizations encountered more than 20 insider-related security incidents annually, with human error contributing to 68% of data breaches.

Background of the Study

A comprehensive and systematic review of the literature revealed three main themes: (a) the influence of impulsivity and privacy concerns on human behavior in cloud business and data security environments, (b) the tripartite relationship between impulsivity, personality, and information security, and (c) the intricate intersections of personality versus privacy (Jawinski et al., 2021; Lee et al., 2020). Upon further research, some scholars (Horwood & Anglim, 2021; Lee et al., 2020) have contrasted specific categorizations within these overarching themes, focusing on the different aspects of the intersectional construction of personality and behavior.

On the other hand, the final investigation of personal learning models was characterized by introducing an innovative theoretical perspective that effectively revealed previously unexamined aspects of the intricate relationship between personality and cultural background (Lee et al., 2020). Highhouse et al. (2022) proposed novel personality antecedents as potential moderators that may have combined drivers in the relationship between personality and privacy concern. This statement was based on empirical evidence that risk propensity and impulsivity were strongly associated with personality constructs, but retained their own identities

(Jochemczyk et al., 2017; Highhouse et al., 2022). For example, Buelow and Cayton (2020) embarked on an empirical journey to uncover the associations between the Big Five personality traits (e.g., extraversion, agreeableness, openness, conscientiousness, and neuroticism) and outcomes within risky decision-making tasks, underscoring the personality predispositions that govern decision-making procedures. In a parallel vein, Indrajaya (2022) observed that individuals displaying heightened levels of extraversion, conscientiousness, and neuroticism were predisposed toward impulsive purchasing behaviors, especially in digital domains. Such behaviors might be symptomatic of a deeper personality configuration that occasionally tends toward impulsivity. On the contrary, Garcia-Argibay (2019) highlighted that negative senses are due to the pronounced impact of neuroticism personality and correlated with a diverse range of behavioral deviations, which led to drug addiction.

Although the literature presented insightful findings regarding impulsivity, personality traits, and behavioral domains, some scholars (Horwood & Anglim, 2021; Lee et al., 2020) refrained from mapping the theoretical relationships between impulsive behaviors and personality. Thus, the current research strived to bridge the gap and bring scholars' attention to why investigating interrelated relationships between impulsivity, information privacy, personality, and security behavior was critical for future literary enrichment and practical applications in cloud business and data security management. Furthermore, the researcher reasoned that most data breaches were in the cloud security domain (Faro, 2023), and this amplified the need to delve into the core of the cloud business and security domain to explore the behavioral factors hindering business performance. With a literary lens, this research was bound to bring compelling insights and a distinctive voice to the existing literature, representing under-

researched realms of cloud business and data security with a core focus on the complementary relationship between impulsivity and individual behavior.

Statement of the Problem

The business problem addressed in this study was that human errors led to data security breaches, resulting in significant revenue loss in the cloud business. Aivazpour and Rao (2022) examined the role of impulsivity and concluded that motor impulsivity directly influenced the extent of information disclosure and moderated the relationship between privacy concerns and disclosure behaviors. Another study on motor impulsivity emphasized the effectiveness of automated monitoring techniques in assessing impulsive behaviors (Dalimarta et al., 2025). Cui et al. (2023) examined the moderating effect of openness to experience on the relationship between team cognitive diversity and innovative work behavior, revealing that openness moderated the relationship between cognitive diversity and knowledge sharing, thereby influencing innovation in workplace settings. It is also the cost of downtime, which often results from human error and is estimated to be as much as $400 billion annually for larger organizations (Bradley, 2024). Humans still matter in massive incidents of cloud business and data security breaches (Clifton, 2024; Snipes, 2024).

Recognizing individuals' dynamic personalities, impulsivity, and behavior was crucial for enhancing cloud business strategies and security management in digital environments (Ding et al., 2024). The explorations and investigations from various scholars (Aivazpour & Rao, 2022; Cui et al., 2023; Bradley, 2024; Clifton, 2024) warranted further investigation into how personality traits interact with impulsivity in shaping cloud business and data security risks. Similarly, Dornheim and Zarnekow (2024) noted that without a comprehensive understanding of the factors that lead to security breaches and incur post-breach losses, every organization faces

significant challenges in detecting insider threats, responding effectively to security breaches, and managing access to sensitive information. Jamieson et al. (2023) further explained that every business enterprise must close the security policy and training gaps to reduce the likelihood of unauthorized access, data leaks, and operational disruptions. They further cautioned that data security vulnerabilities restricted business scalability and revenue streams, with underlying human errors being the impediments to maintaining customers' trust, ensuring data privacy compliance, and ensuring technology stability in an increasingly complex digital landscape. Therefore, the problem this study addressed was the lack of understanding of the relationships between impulsivity, personality traits, and behavioral dynamics that are important for enhancing cloud security processes and business continuity, customer confidence, and shareholder value.

Purpose of the Study

The purpose of this study was to explore the direct impact of motor impulsivity on individual behavior, the chain mediating role of personal information privacy (PIP), and the moderating role of openness to experience (OE) personality trait (Big Five personality traits) on the connection between motor impulsivity and individual behavior in cloud business and data security management. The independent variable explored was motor impulsivity, and the dependent variable was individual behavior; the mediators and moderators were personal information privacy and openness to experience. The intended audience was business and security-related professionals who were familiar with cloud data. The sample consisted of 150 individuals, and the survey participants had over 5 years of experience in cloud business and data security. Data was collected through a Qualtrics digital survey, incorporating multiple validated instruments to assess key study variables. The survey comprised demographic variables, such as participant profile, and standardized assessments of personality and behavioral phenomena.

Motor impulsivity was evaluated by a scale set up by Coutlee et al. (2014), and openness was assessed using the widely used measure by Rammstedt & John (2007). Personal information privacy was measured following the model by Smith et al. (1996), and the individual behavior of cloud business and data security was assessed by means of scales proposed by Parsons et al. (2014). This study also provided suggestions for the measurement component of personality, like openness to experience, the moderation effect, and the mediation effect of personal information privacy, which play a role in the relationship between motor impulsivity and individual behavior in cloud business and data security environments.

Significance of the Study

The current study had several potential implications and contributions for business pragmatics and research knowledge. For business practice, the findings of this study have important implications. Partially at the level of the relationship between motor impulsivity and individual behavior, the mediating role of personal information privacy, and the moderating role of one of the Big Five personality traits, openness to experience is the point; controlling the privacy paradox and impulsive behaviors of the participants is an important milestone, especially since the organizations were facing an increasing number of cyber security threats. Organizations should thus address technical and institutional solutions to prevent and control the risks (Alrashdi, 2023).

This study promoted Aschwanden et al.'s (2024) conclusions that security behaviors were deeply rooted in personality traits and privacy factors outside of policy enforcement, besides advancing literature and oration contributions. In addition, recent research added a behavioral dimension to this field by incorporating a behavioral dimension of cybersecurity into predictive cybersecurity models (Faschang et al., 2024). The significance extended to artificial intelligence

applications and predictive analytics, which could identify impulsive real-time security behaviors and provide personalized recommendations to users, laying the groundwork for future AI-driven interventions, strengthening cloud security resilience, and reducing human error (Khan et al., 2025).

Research Questions

This correlational quantitative study used a sample of 150 cloud business and data security professionals to examine two key research questions. The two questions were as follows:

RQ1: Does motor impulsivity impact individual behavior in cloud business and data security management?

RQ2: How does privacy of personal information mediate, and how does the Big Five personality trait of openness to experience moderate, the relationship between motor impulsivity and individual behavior in cloud business and data security management?

Hypotheses

The hypotheses for the research questions enumerated above were null and alternate hypotheses and were aligned with two main research questions.

$H1_0$: Motor impulsivity does not significantly impact individual behavior in cloud business and data security management.

$H1_a$: Motor impulsivity significantly impacted individual behavior in cloud business and data security management.

$H2_0$: Personal information privacy does not significantly mediate the relationship between motor impulsivity and individual behavior in cloud business and data security management.

$H2_a$: Personal information privacy significantly mediated the relationship between motor impulsivity and individual behavior in cloud business and data security management.

$H3_0$: Openness to experience does not significantly moderate the relationship between motor impulsivity and individual behavior in cloud business and data security management.

$H3_a$: Openness to experience significantly moderated the relationship between motor impulsivity and individual behavior in cloud business and data security management.

Assumptions

According to Creswell and Cresswell (2017), the blueprint for a quantitative study is to confirm hypotheses with empirical indicators and quantitative data, as well as the theoretical methodologies required to verify or falsify inferences. Consequently, the investigator employed a quantitative research design, including a correlational type, to systematically examine hypotheses and statistical procedures. The study's correlational nature allowed for the investigation of the associations among motor impulsivity and individual behavior, moderated by openness to experience, one of the Big Five personality traits, and mediated by personal information privacy, without manipulating the variables (Watzlaf et al., 2015). The implications of the results of this quantitative research design, as regards the intricate interplay of these variables in cloud business and data security management, are based on the following assumptions:

1. Respondents answered the Qualtrics survey honestly without much personal bias.
2. The operationalizations for motor impulsivity (Coutlee et al., 2014), openness to experience (Rammstedt & John, 2007), personal information privacy (Smith et al, 1996), and individual behavior (Parsons et al., 2014) were believed to measure the intended constructs validly and reliably.

3. Moderating and mediating effects are the elements and tendencies of open-mindedness and personality in the relationship between motor impulsivity and personal behavior, which are significant and expected. Meanwhile, personal information privacy is a crucial mediator in this association.
4. Multiple regression analysis, a statistical procedure that was appropriate to test for the relationships among the independent, dependent, moderator, and mediator variables, was conducted, and the sample size was expected to be large enough to yield a statistically strong conclusion.
5. The organizations knew and expected the employees' behavior based on risk propensity.
6. Although organizational policies, cybersecurity training, or previous risk exposure could affect user responses, the assumption was that the organizational size does not dominate the investigated variables.
7. Following additional research (Goel et al., 2019), it was hypothesized that there was an association between impulsivity and risky behavior.
8. The study findings from impulsiveness, openness to experience, and personal information privacy impacts on individual behavior can be used to enhance cloud security policy and business management.

Definitions of Terms

Big Five personality traits, the five-factor model (FFM), is the framework for assessing human personality and referred to as the five-factor model of personality, or OCEAN: openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism (Zhang et al., 2024).

Cloud business and cloud security: Cloud business is described as using cloud computing solutions to create digital transformations (Alves, 2023). In contrast, cloud security entails the strategies, technologies, and policies to protect cloud architectures from cyber-attacks, data loss, and intrusion attempts (Ahmadi, 2024).

Cybersecurity: Cybersecurity is the strategic implementation of protective measures designed to defend systems, networks, and data security against cyber threats, unauthorized credentials, and malicious attacks (Dornheim & Zarnekow, 2024). By safeguarding sensitive information, cybersecurity plays a vital role in preventing breaches, mitigating risks, and reinforcing the resilience of modern digital environments (Craigen et al., 2014).

*Human aspects of information securit*y: Focus on human behaviors, decisions, and actions that can influence information security (Voss, 2023). It emphasized understanding how users interact with systems and the potential vulnerabilities that can arise (Dhillon & Torkzadeh, 2006).

Information security: The practices and principles of protecting information from unauthorized access, use, disclosure, disruption, or destruction. It encompasses physical and digital data protection methods (ISO & IEC, 2022).

Insider Threat: According to Dalal and Gorab (2016), insider threats are the risks caused by organizational resources like employees, contractors, or business partners who misuse their authorized access to systems, networks, or data, either intentionally or unintentionally, in a way that could harm the organization.

Impulsivity: Refers to actions without forethought and a personality trait that urges to act on a whim without deliberation or consideration of the consequences (Moeller et al., 2001).

Personality: Demaree et al. (2005) described personality as a complicated portrayal of an individual whose thinking patterns, sentiments, and behaviors were consistent over time and context.

Phishing: A cybersecurity attack where disguised hackers force online users and organizational members to reveal confidential, personal, and business-sensitive information (Zhang, 2025). The deception tactics look very authentic in that the individuals are easily exploited through emails, counterfeit websites, or misleading communications, ultimately leading to unauthorized access to sensitive data (Cybersecurity & Infrastructure Security Agency, 2023).

Privacy concerns: Refer to individuals' apprehensions about losing control over personal information and the potential for unauthorized access to or misuse of this data (Smith et al., 2011).

Social Engineering: According to the National Institute of Standards and Technology (2025) glossary, **"**An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks" (p. 60).

Organization of the Dissertation

Chapter 1 of this dissertation introduced impulsivity, personality, information privacy, and behavioral implications, drawing potential connections to insider threats and data breaches. Then, the problem was stated, along with the purpose and significance of the study, sourcing relevant literature to recognize the knowledge gap in cloud business and data security management. Furthermore, suggestive contributions and centered research questions clarified the focus of the research and its objectives, while an outline of the remaining chapters was drawn. Chapter 2 incorporated the literature review within the broader context of impulsiveness,

information privacy, personality traits, and individual behavior and relationships, which were systematized in a thematic format. The review was initiated by outlining the literature search strategy and the study's theoretical framework, including the risk propensity model (RPM) and the Big Five personality characteristics. The main themes explored in the literature included motor impulsivity, personality type, openness to experience, and personal information privacy as influencers of human behaviors in cloud business and data security management.

Chapter 3 described the quantitative research design, population criteria, random sampling, reliability and validity, instrument development, and data collection, and considered ethical obligations. Additionally, data analysis procedures and the broader impacts of the study were highlighted. The statistical results were illustrated in Chapter 4, and the data standardization procedures were documented, as well as descriptive and inferential statistics and hypothesis test results. Chapter 5 discussed the hypotheses' results, and their applicability to the theoretical context in the dissertation's literature review; future research recommendations and study limitations were noted with valuable insights and contributions to cloud business and data security management.

Chapter 2: Literature Review

The purpose of this study was to investigate the direct impact of motor impulsivity on individual behavior, to the extent to which openness to experience, a Big Five personality trait, moderated the relationship between motor impulsivity and individual behavior, with personal information privacy serving as a mediating factor in the context of cloud business and data security management. Within cloud business and data security, a subset of the cybersecurity profession, information security and privacy are widely recognized as fundamental values (Pawlicka et al., 2022). Once organizations started to leverage cloud computing solutions for both scalability and cost effectiveness, security became an integral part of their end-to-end cloud business and their respective data security and cybersecurity methodologies for safeguarding against threats in current digital environments (Craigen et al., 2014). Because motor impulsivity has been reported to affect the way how people participate in social impulsivity, Big Five personality traits corresponded to impulsivity (Indrajaya, 2022) and were found to manage private data (Aivazpour & Rao, 2020). Big Five personality traits and impulsivity relations with individual behavior comprised the present study, which examined the interplay of such constructs and their influence on cloud business and data security management.

The literature review involved an in depth study on impulsivity, privacy concerns, Big Five personality traits (openness to experience), and their importance in explaining human factors impacting cloud computing and information security in the cloud business and data security domain. This chapter commenced with a description of the search strategy in the literature that had been developed, which followed presentation of the specific search engines utilized, search terms utilized to search for publications, and criteria for evaluating relevance and credibility for all search results; then qualified the theoretical grounding of this work in the

discussion about tendency to take risks model (RPM) has been instrumental in forming the research. Specifically, the RPM facilitated the connection between the Big Five Personality traits and impulsivity, a linkage essential for exploring the moderating effects of these traits on the relationship between impulsivity and privacy concerns within the cybersecurity domain. Following this, the researcher delved into the main body of the literature review, which was organized into three key themes. The first theme addressed impulsivity and privacy concerns as influencers of human behaviors in cloud business and data security roles. The second theme explored the contribution of impulsivity to the interaction with personality and information security. The third theme investigated personality and privacy. The discussions comprehensively addressed the study variables, including motor impulsivity, personal information privacy, openness to experience, and individual behavior, and focused on the most important relationships among them. As the literature overview identified, a key gap in the research was determined, highlighting the importance of future research to fill this gap. The chapter was closed with a recapitulation of the main points presented, offering a cohesive summary of the insights gained through the literature review.

Literature Search Strategy

To retrieve articles for this study, the researcher utilized the Franklin Library, including Ohio Link, providing access to theses and dissertations from students at 31 academic institutions in Ohio, making it a rich resource for academic research. ProQuest was another offering of Franklin Library, with curated content aligned with academic curricula and advanced search tools to support the investigators. Electronic Journal Center, Google Scholar, and Emerald Insight databases were primary sources for retrieving literature on cloud business, cybersecurity, and personality traits related to impulsivity, individual behavior, and privacy concerns. The

Google Scholar database was helpful because it included sources across the entire cloud business and data security, including sources from scholarly journals, professional conferences, and websites that contained acceptable sources. One risk of using this search engine was that it was necessary to use effective filters to ensure that only genuinely scholarly sources were accepted for this review, instead of various other sources that may have been included in the search hit from across the cloud. The Emerald Insight database was helpful because it focuses specifically on more professional disciplines, including disciplines such as cybersecurity and psychology. By searching these two databases, the researcher retrieved sources on all the topics of interest for this literature review.

The search terms for the literature search were derived from the primary constructs of the selected topic, including privacy concerns, impulsivity, cybersecurity, privacy practices, personality, information security, risk propensity, and the Big Five personality traits. The researcher conducted the literature review by running searches using various permutations of these concepts. For example, one search included privacy concerns and impulsivity, and another included impulsivity and personality. I retrieved approximately 90 articles for this literature review through these searches of the selected databases. When each article was retrieved, the titles and abstracts were examined to ensure that the article in question was appropriate for inclusion in the present literature review. The researcher was thus finally responsible for all of the articles included in the study and did not depend only on the search engines themselves to produce credible results.

In addition to this manual examination of retrieved sources, the researcher also established parameters during the search. Two main parameters were important in this regard. The first consisted of establishing year limits so that most of the articles retrieved were published

within the past 5 years. However, this filter was turned off for the search regarding the theoretical foundation section, since it was important for that section to retrieve older and seminal sources to gain a sense of development over time. The second parameter required that only scholarly sources be retrieved through the search. The search was driven by the search terms alone, and the main themes and categories of the literature review were developed afterward through an analysis and synthesis of the sources retrieved through the search process. The main themes were designed to emphasize the focus on cybersecurity and the interrelations among the variables of impulsivity, privacy, and information security. Three main themes emerged, and within each were two subthemes, together creating the structure of the body of the review. Such interconnection was inevitable, given the subject matter, though the researcher endeavored to differentiate them sufficiently to ensure that each debate formed around a distinctly different issue.

Theoretical Framework

The entire study was based on the RPM as its theoretical framework. No single theorist can be credited for how the RPM came about; instead, it evolved due to studying the root of the construct of risk propensity. Sitkin and Pablo (1992), for example, introduced risk propensity as a critical determinant for how individuals assessed the levels of risk in a situation (either real or imagined) and how they reacted to it—implicitly or explicitly—those perceptions. Nicholson et al. (2005) built on this research by linking risk propensity to personality, finding that certain personality traits were significantly associated with increased odds of risk-taking behavior. Zhao and Seibert (2006) also assisted in developing the RPM by examining the connection between Big Five personality traits and entrepreneurs' status, which was used as a proxy for risk propensity. Their findings revealed that individuals with greater risk propensity exhibited distinct

personality traits compared to those with lower risk propensity. This body of work collectively facilitated the evolution of a comprehensive model linking risk propensity with personality traits, culminating in the conceptualization of the RPM employed in this study. The RPM was closely connected to the General Risk Propensity Scale (GRiPS), which served as the primary empirical tool for measuring risk propensity and was validated as reliable within the relevant scholarly literature (Meertens & Lion, 2008; Zhang et al., 2018).

The RPM focused on linking risk propensity with personality traits. The GRiPS provided an effective method for empirically measuring risk propensity. At the same time, the Big Five personality traits, well-established in scholarly work, had a long history of being measured in valid and reliable ways (von der Linden et al., 2010). Thus, both core elements of the RPM were amenable to rigorous empirical measurement within this study. The findings further supported the assertion by Highhouse et al. (2022) that risk propensity was significantly independent of the constructs of the Big Five factors. This independence indicates that risk propensity cannot simply be reduced to or treated as a direct function of these personality traits. On the contrary, RPM served as a sound theoretical and empirical framework in this study, in that it allowed us to integrate two different variables, risk propensity and personality, without confounding them (Lee et al., 2020). This differentiation highlighted the necessity of using a tool such as the RPM to look at these variables in a more integrated and valid way for the current study. Subsequent research has reinforced the notion of a risk tendency construct and its relationship to the RPM (Jochemczyk et al., 2017). For example, Zhang et al. (2023) examined the pros and cons of involvement with risk-takers. Their results indicated that risk-takers may have negative traits according to the Big Five and are expected to practice counterproductive work behaviors than non-risk-takers. The impact of organizational whistle-blowing on the atmosphere of an

organizational value and citizenship behavior (Miglin et al., 2019). However, the positive side was that a risk taker frequently adds to the success of an organization in breaking ineffective rules, introducing innovation, or helping an organization learn and find solutions that reach beyond existing operational limits (Mirsch et al., 2017). This double-faced nature of the behavior of the risk-takers backed important implications for the cloud business and data security context. In a second study, Jochemczyk et al. (2017) studied the interaction between risk propensity, personality traits, and time perspective. Pawlicka et al. (2022) found that time perspective, an individual's inclination to operate in the present moment versus the future, was a stronger predictor of risk propensity than personality traits.

In other words, risk takers among the professionals were the people who were conscious about living in the here-and-now, which was supported by the conclusion of Highhouse et al. (2022) that risk propensity was an independent construct, distinct from personality traits, which must be regarded as a separate but connected variable. RPM arises from the interpretation that, naturally, unified the linking between personality traits and the risk without mixing and confusing them (Peterka-Bonetta et al., 2019). Furthermore, these insights supported the theoretical basis of the present study by considering various interrelated factors and further assuming personality factors as moderators of risk.

Before the literature review was continued, it was worth briefly discussing that the Big Five personality model had much to do with this study. The Big Five personality traits—openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism—are widely recognized and commonly referred to as the OCEAN model, an acronym of these traits (Rothmann & Coetzer, 2003). Unlike many other personality assessments, the Big Five model has confirmed validity and reliability in the relevant literature, which accurately empirically

measured existing personality traits (Zhang et al., 2018). This study used the Big Five model to define personality traits, and risk propensity was defined using the GRiPS. Similarly, privacy concerns, particularly regarding personal information, play a significant role in shaping individuals' behaviors and decision-making processes, which are central to the RPM. Personal information privacy refers to individuals' apprehensions about how their data was collected, stored, and used, especially in digital environments (McClain et al., 2023). According to McClain et al. (2023), risk played a significant role in people's perceptions when asked to consider the potential benefit (information sharing) versus cost (the possible misuse or unauthorized access to the information). For example, research by Sichel (2021), Ji (2022), Musafiri Mimo (2022), and McClain et al. (2023) has evidenced that individuals with higher levels of privacy concerns were more likely to take protective measures to reduce information disclosure or make use of privacy-protecting tools. This supported the RPM argument that risk propensity was influenced by personality differences and situational factors, like privacy concerns, that affected people's perceptions of and responses to risk (Lee et al., 2020).

RPM Application and Framework

The RPM was particularly suitable for the current study because the present study regarded personality traits as moderators, impulsivity as a precursor, and privacy concerns as a mediator. The RPM offered an important paradigm to explore how privacy concerns, like personal information privacy, interact with impulsivity, influencing business risk-taking behaviors, where high conscientious students might have higher sensitivity to privacy risks, leading to conservative trade-offs, and open students might favor innovation and tolerate higher privacy risks (Merians Penaloza, 2024). Privacy worries were not monolithic but were subject to strict dependence on cultural factors, technological literacy, and experiences of previous data

breaches, which have also emphasized research (Rousseau, 2024). Hwang (2024) suggested that by incorporating privacy into the RPM, scholars would be in a stronger position to grasp the subtle and indirect manners in which privacy impacts risk propensity, thereby guiding the development of effective privacy laws and system protection processes. According to the RPM, motor impulsivity was a precursor for risk behavior because it impacted how risky situations were perceived and dealt with (Jochemczyk et al., 2017). Individuals with high motor impulsivity tendencies were more likely to engage in risky actions, as they may be more willing to act than think before they act (Highhouse et al., 2022). This was consistent with the RPM's definition of risk propensity as an attribute of an actor. In contrast, the subjectivity or purely cognitive interpretation of risk propensity occupied one of the endpoints of the dimension. Proclivities and perspectives influenced their broader attitude toward risk (Rizki et al., 2022).

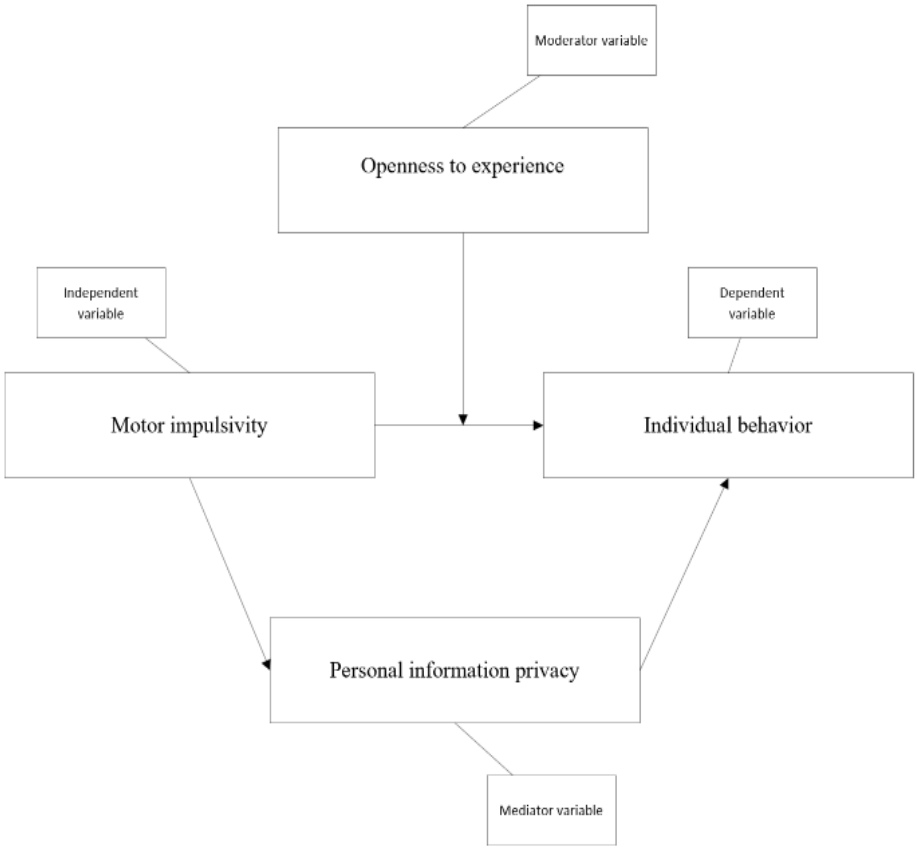
Motor impulsivity was the main factor in understanding how particular persons were before experiencing any thrill or newly discovered sensation, because of a reserve of energy in a race against time—risk-prone across domains, such as cybersecurity and information management (Ana, 2024). Furthermore, the RPM's connection between personality traits and risk propensity provides a valuable lens for examining the role of motor impulsivity. RPM's ability to integrate these nuanced interactions made it an ideal framework for conceptualizing motor impulsivity, not as an isolated variable, but as one that interacts with personality traits and privacy concerns to influence human behaviors in situations that involve risk, such as cloud business and data security (Hadlington, 2017). Thus, RPM served as the conceptual and analytical framework and robust foundation for this study, effectively connecting intricate relationships of openness to experience and personal information privacy and motor impulsivity with risk propensity.

Conceptual Framework

The RPM proved highly relevant to this study as it conceptualized the personality trait of openness to experience as a moderator, motor impulsivity as an antecedent, and personal information privacy as a mediator. This framework in Figure 1 successfully linked the study variables, enabling an exploration of their combined influence on motor impulsivity and the resulting individual behavior outcomes in cloud business and data security management.

Figure 1

Conceptual Model



Note. The tripartite relationship between the predictor, mediator, moderator variables influencing the outcome is demonstrated in the conceptual framework.

The study's conceptualization represented a viable connection among these variables, with the causal chain from motor impulsivity to individual behavior. Within this chain, personal information privacy functioned as a mediating variable, while openness to experience was a moderating variable. Given that the RPM was not a fixed model but a flexible analytical tool, it was an excellent theoretical foundation for this study. By intertwining and cross-linking these constructs, the researcher was able to understand the relationship between these constructs and how personality traits, impulsivity, and privacy concerns work together to shape behaviors. This flexible structure strengthened the researcher's power to answer the research questions and generate knowledge, which is very valuable to the field for cloud security management in business and data. This dynamic framework reinforced the study's ability to address its research objectives and contribute valuable knowledge to cloud business and data security management.

Furthermore, RPM broadly asserted a connection between risk propensity, personality traits, and other related variables. However, existing literature indicated that risk propensity was not directly caused by personality traits, a topic that was explored further in subsequent discussions. For this study, the approach reflected a legitimate and well-grounded use of the RPM, rooted in an understanding of literature on the evolution of the risk propensity construct over time. In the literature review, three main categories were emphasized: 1) the association between impulsivity and the individual's behavior; 2) the interplay of impulsivity, personality traits, and behavioral patterns; 3) the contribution of impulsivity to privacy concerns and the individual's decisions. These themes provided the foundation for examining the two central research questions.

RQ1: Does motor impulsivity impact individual behavior in cloud business and data security management?

RQ2: How does privacy of personal information mediate, and how does the Big Five personality trait of openness to experience moderate, the relationship between motor impulsivity and individual behavior in cloud business and data security management?

The research questions presented are grounded in the conceptual framework of this study, and the main topics of the literature review are derived from the constructs within that framework and the research questions. This section has effectively established the interconnections between motor impulsivity, privacy concerns, personal information privacy, and individual behavior within the broader context of cloud business and data security management. Notably, the second topic of the review delved into the relationships among motor impulsivity, openness to experience, and individual behavior.

Review of the Key Literature

The structure of this literature review was designed to intertwine the discussions across the three main topics: 1) impulsivity and individual behaviors, 2) impulsivity and privacy concerns influencing individual behaviors, and 3) impulsivity, personality, and individual behavior relationships in cloud business and data security management, forming a cohesive and interwoven narrative. Each theme maintained its separate focus, but deliberate overlap was created to illustrate relationships between the themes to yield an integrated picture of the variables. A braided style was well-suited to this study's complicated framing to ensure that the central concepts' relationships were examined, shaken out, and put into context.

Impulsivity and Individual Behaviors

Impulsivity related to personality was characterized by the ability to make hasty, unplanned decisions, which was a big deal and may have a profound, if not fatal, impact on the cloud business and data security governance (Gilliam et al., 2020). They also demonstrated that

impulsive people were more likely to engage in risky online behaviors, such as sharing personal details, failing to adhere to cybersecurity best practices, and getting caught in phishing scams. Similarly, Diotaiuti et al. (2022) contended that impulsive tendencies are particularly concerned in cloud-based systems, where instant access and ease of data sharing can intensify impulsive decision-making. However, Demircioglu and Kose (2022) suggested that impulsivity interacted with Big Five personality traits, such as openness to experience and conscientiousness, which shaped digital security behaviors. McElroy and Dowd (2023) indicated that individuals who scored high in impulsivity and low in openness to experience and conscientiousness were more likely to disregard security protocols, making cloud systems vulnerable to breaches.

Cloud business models relied heavily on user autonomy, which was problematic when impulsivity drove security lapses (Dezhkam et al., 2022). Research indicated that impulsive individuals were likelier to ignore multi-factor authentication, reuse weak passwords, and engage in unauthorized data transfers, which heightened cybersecurity risks (Durodolu, 2016; Nasirpouri Shadbad, 2021). Given the dynamic nature of cloud systems, businesses failed to consider behavioral interventions alongside technical security measures to mitigate impulsive decision-making (Rousseau, 2024). Cremer et al. (2022) found that cloud business and data security management professionals with high impulsivity favored aggressive security measures, while those with lower impulsivity adopted conservative approaches. Collier (2023) mentioned that cybersecurity professionals exhibited varying risk propensity levels, influencing their cloud business and data security decision-making strategies. Understanding individual behavioral differences improved team dynamics and risk assessment models, ensured balanced cybersecurity strategies within cloud businesses, but the structural design of cloud platforms unintentionally encouraged impulsive behaviors (Babar, 2024). Suntwal et al. (2025) affirmed

that interfaces optimized for speed and ease of access inadvertently promoted impulsive user actions, such as clicking through security warnings without scrutiny. Ana (2024) noted the importance of cognitive interventions that helped users learn to recognize when they were acting impulsively and to stop and think before doing something risky on-screen. Musafiri Mimo (2022) explained that motor impulsivity is exhibited when an individual acts first before having a chance to process the information, which affects how users interact with cloud-based applications and systems.

Additionally, Musafiri Mimo contended that the ad hoc users clicked by mistake on rogue links (in accordance with a cloud or other service provider scenario), bypassed security warnings, or allowed too quickly some access without validating the entity. Voss (2023) explained how hasty, impulsive behaviors increased vulnerabilities within cloud business and data security domains, making data breaches and unauthorized access more likely. Furthermore, the fast-paced nature of cloud business application systems, where efficiency and ease of access are prioritized, led users to react instinctively rather than thoughtfully and amplified impulsivity (Clifton, 2024).

Motor impulsivity impacted cybersecurity risk management, particularly in decision-making processes related to cloud business and data security settings (Yasin et al., 2024). According to Aschwanden et al. (2024), motor impulsivity was a primary factor in social engineering attacks, which led subjects to be conned into violating their own security through social interactions. Their findings revealed that cybercriminals often exploited impulsive behaviors by sending phishing emails, fraudulent cloud access requests, or fake authentication alerts, prompting users to act without carefully evaluating authenticity. Nonetheless, cloud business and data security professionals who failed to pause and assess the legitimacy of such

requests due to impulsivity were at a higher risk of falling for security threats (Dornheim & Zarnekow, 2024). Cloud business models lost focus on detecting insider threats and designing behavioral cybersecurity training that would have taught users to recognize impulsive reactions and encouraged adopting intentional security practices (Georgiadou et al., 2022).

The privacy paradox, which was referred to as a disconnect between individuals' stated concerns about privacy and their actual online behaviors about data security, but engaged in risky behaviors, was linked to impulsivity (Al-Nuaimi, 2024). The privacy paradox, known as the hiatus between people's stated concern for privacy and online privacy behaviors, involved various risky behaviors and was associated with impulsivity (Al-Nuaimi, 2024). However, Burton et al. (2023) posited that individuals with high impulsivity often lack intent-behavior congruence, thus exhibiting inconsistent privacy management. According to Sadeghi et al. (2023), privacy paradox in cloud business entails personnel who clicked on suspicious links or saved personal details at unsafe locations based on convenience and temporal decision making.

Summary. In this section of the literature review, I presented the influence of impulsivity on individual behavior in cloud business and data security management. Specifically, I concentrated on how a personal psychological trait, such as the motor impulsivity domain, led to cloud business and data security vulnerabilities. The key takeaway revealed that impulsive people were likelier to exhibit dangerous digital behavior, including ignoring cloud security best practices, sharing sensitive data with those they should not, and clicking on suspicious links in emails or websites without proper due diligence. Furthermore, the privacy paradox, whereby users expressed privacy concerns yet engaged in actions that contradicted their privacy, demonstrated the challenge of aligning intuitive-based decision-making with sound practices of cloud business and data security. Therefore, the privacy paradox has highlighted the significance

of adaptive security interventions that help override impulsive dispositions regarding cloud business and data security environments. Most importantly, the conversation in this section brought forward the role of motor impulsivity in forming cloud business and data security professionals in the digital security landscape. Threats, especially in cloud-based communication, and the importance of understanding the privacy paradox phenomenon by integrating motor impulsivity with individual differences.

Impulsivity and Privacy Influence on Human Behaviors

This part of the literature review concentrated on the impulsive characteristics and privacy concerns as a significant role in stimulating individuals' behavior in cloud business and data security. It was categorized based on impulsivity, privacy concerns, human factors, and data security in the cloud business. A central theme that developed from this discussion was privacy. Paradox phenomena illustrated the dissonance between people's expressed attitudes toward privacy, on the one hand, and their actual behaviors, on the other, when it comes to interacting with the cloud and other digital platforms.

The privacy paradox highlighted a dichotomy between purposeful, reflective considerations of privacy and impulsive actions that undermine privacy in the heat of the moment in naturalistic circumstances. It also considered the implications of the privacy paradox in cloud business and data security, how it applies to business as usual, and the challenges confronting business and technology professionals. They protect users' privacy and counteract impulsive behaviors that subvert security procedures. By examining these processes, this section has offered invaluable predictors of interactions in which impulsivity and privacy concerns impact security-related behaviors, since not only cloud business but also data, obligation, and accountability security are all dynamic.

Impulsivity and Privacy Concerns

The privacy paradox, which concerns impulsivity and privacy, was widely discussed in the literature and explained how individual professionals can say they value protecting their privacy but act in ways that are at odds with that value. According to Aivazpour and Rao (2020), motor impulsivity played a significant role in this paradox, as it can lead individuals to behave in ways that contradict their stated values regarding privacy. Similarly, Mantilla and Robles-Flores (2021) found that individuals with higher levels of risk aversion tend to be less influenced by the privacy paradox when engaging with the cloud business and data security, suggesting that aversion to risk served as a protective factor against impulsive privacy-compromising behaviors. Goel et al. (2019) also pointed to the role of motor impulsivity in the privacy paradox, as people might weigh short-term gains versus long-term costs differently; those higher in impulsivity are more likely to push for immediate gains, regardless of the long-term implications of revealing their privacy.

Ji (2022) further supported this by emphasizing that impulsive individuals are less likely to weigh future costs. Waranowicz (2024) contrasted this with less impulsive individuals, who take long-term consequences into account and adjust their behavior accordingly. Impulsivity emerged as a key driver of actions that can compromise an individual's personal business-related privacy. In this context, impulsivity can be closely aligned with risk propensity, as impulsivity often involves a greater willingness to take risks, specifically the short-term disregard for privacy risks in favor of immediate rewards. In their research, Alashoor et al. (2022) found that people cared less about privacy when exhausted or in an elevated mood. According to Flores (2016), being tired, for example, can negatively affect impulse control, and an elevated mood could also make one less attentive to the potential negative consequences of one's actions in the present. In

another study, Ioannou et al. (2021) found that dispositional mindfulness may serve as an antecedent to privacy concerns. This finding was logical, given that dispositional mindfulness likely has a significant connection with impulsivity, such that the greater the dispositional mindfulness of any given person, the lower their impulsivity.

Moreover, Durodolu's (2016) research suggested that the cloud was often designed to make people more impulsive and thus more likely to ignore their declared individual and organizational privacy concerns. This practice was sometimes known as digital nudging, and it involved providing users with implicit or explicit encouragement to be more impulsive (Mirsch et al., 2017; Adjorjan & Ricciardelli, 2019). This point calls attention to the fact that actors in the cloud business and data security who are aware of the privacy paradox can behave in predatory ways to pursue their interests by undermining cloud users' concerns about privacy or their willingness to control their impulses in alignment with those concerns. Diotaiuti et al. (2022) discussed cloud addiction, which was quite relevant to the present discussion. According to these researchers (Blaschke, 2019; Adorjan & Ricciardelli, 2019), greater impulsivity and codependency can catalyze cloud access addiction, just as they could potentially catalyze addictions of various kinds. For present purposes, however, one must also consider that addiction could radically increase impulsivity in terms of the privacy paradox. When a person is addicted, the strength of their will is significantly compromised, and they will likely do whatever is required to obtain the object of their addiction, even if doing so means compromising their values. In this context, if people value privacy, they are also addicted to cloud applications (Lin et al., 2016). They would almost certainly compromise the value of business and personal information privacy to obtain access to various cloud business and data security areas or engage with various services. Lyvers et al. (2021) also studied cloud addiction and impulsivity, and a

similar implication can also be drawn from that research. In this context, the practice of digital nudging became particularly insidious insofar as it could be a way to catalyze Cloud addiction, influencing working employees in the cloud business and data security (Le, 2019). According to (Lembcke et al., 2019), greater impulsivity led to diminished practical concerns of privacy, but also that social engineering agents on the cloud market may be aware of this fact and thus try to increase impulsivity of the employees, with the result that those agents could more easily manipulate cloud business users. The empirical evidence largely supported the existence of the privacy paradox, although different studies in the literature posit different specific conceptual relationships between various factors underlying the paradox.

For example, Barth et al. (2019) found that business application users typically take several considerations into account, such as the ease of using the application or the relative cost versus benefit of using it. Such findings suggest a high level of impulsivity in the first place, such that the paradox was somewhat dissolved as a paradox per se through users simply being so impulsive that they no longer think very much about privacy. Such dynamic, however, would be very problematic, because as Nedelec (2018) has indicated, people with higher impulsivity in both online and offline settings report greater levels of victimization. Therefore, one could draw the implication that cloud business and data security users today are being primed for high levels of victimization as they become either less mindful of privacy, even in theory, or less active regarding their privacy concerns in practice. While the privacy paradox may be difficult to model in rigorous terms accurately, Hirschprung et al. (2022) have made efforts in this regard using soft logic and other mathematical techniques to model the ways that impulsiveness and privacy concerns relate to each other within the context of cloud users' experiences. In sum, it was fair to say that the privacy paradox was 'real'. It described an actual 'gloss-over' among cloud users of

their stated privacy concerns and their implementation of practices substantiating them. Moreover, the privacy paradox often occurs not due to users' behaviors not matching intentions (e.g., people worrying less about privacy) but due to users losing sight of privacy issues. It suggested that privacy concerns were more likely to increase than decrease over time.

According to Ostendorf and Brand (2022), it was misguided to imagine that cloud business and data security users are engaging in a rational calculus of costs versus benefits when they disclose information about themselves. Instead, it is essential to recognize that individuals operate in a digital environment where they are frequently encouraged to disclose personal information from various sources (Voss, 2023). In such a context, it became meaningless to maintain that cloud business and data security users are rational actors. The practice of digital nudging, for example, made this point very clear (Lyvers et al., 2021; Mirsch et al., 2017). Cloud business and data security marketers seek to downplay users' privacy concerns while strategically encouraging them to share personal information (Hadlington, 2017). Furthermore, Briggs et al. (2017) contends that cloud business and data security marketers' approach often involves framing data disclosure as harmless or beneficial, leveraging persuasive techniques to promote engagement while minimizing perceived risks. Such manipulations to disclose data can sometimes be highly manipulative, even when they adhere to legal standards, let alone the actions of hackers and other malicious entities operating beyond those legal boundaries (Khan et al., 2021). Therefore, the privacy paradox presented significant challenges from the information security standpoint. Individuals with higher impulsivity are more prone to risky behaviors that put their data privacy at risk (McElroy & Dowd, 2023). Additionally, digital platforms are often designed to promote impulsive decision-making, further amplifying these vulnerabilities (Zhang et al., 2023). This general context established the importance of the main

topic selected as the focus of the present study's inquiry. It was essential to understand the business privacy paradox better and to work toward mitigating its negative consequences.

Human Factors and Privacy Concerns

Cloud business and data security professionals are concerned with impulsivity and privacy issues (Hwang, 2024). Conceptually, such professionals are called to either help reduce impulsivity or improve privacy protections in a way that considers impulsivity. According to Gillam and Foster (2020), three factors that contribute to enhanced privacy measures among cloud users are 1) perceived susceptibility, 2) perceived cost, and 3) self-efficacy. According to Georgiadou et al. (2022), cloud business and data security professionals' prioritization and time allocation to learn potential risks to the business, cost-effective security measures, and secured cloud application navigation enhancements contributed to the mitigation of insider threats. Burt (2019) indicated that privacy had become a top concern within the cybersecurity discipline, such that the concept of privacy was increasingly converged with the concept of security.

Once regarded as an abstract ethical concept, data privacy has evolved into a more tangible notion of security, emphasizing data protection from unauthorized access and malicious threats (Blevins et al., 2021; Suntwal et al., 2025). Risk propensity varies widely among cloud business and data security professionals, shaping how individuals assess digital threats and determine appropriate responses (Diotaiuti et al., 2022). Differences in risk perception between cloud business professionals and data security experts may significantly impact decision-making and the creation of security measures in the digital realm (Nifakos et al., 2025). According to Cremer et al. (2022), such people are likely to engage in aggressive or proactive security measures, which involve planning for unknown dangers. Conversely, those with a lower risk tolerance may focus on conservative approaches, emphasizing compliance, structured protocols,

and minimizing vulnerabilities rather than proactive engagement (Ahmed et al., 2021; Stewart, 2020). However, Akeiber (2025) illustrated that cloud business and data security professionals must be aware that malicious actors are actively exploiting the privacy paradox to protect cloud users from their personal information. As Li and Liu (2021) noted, most cyber-attacks involve the theft of digital information, and many such attacks involve the cloud business and technology users at least tacitly or implicitly permitting the attackers to access the information in question. Emerging technologies, such as 5G networks, raise further issues regarding matters of privacy and trust (Mazurczyk et al., 2020). Emerging technologies can create new vulnerabilities, meaning that even if users maintain consistent levels of impulsivity and privacy awareness, the overall risk to privacy may still rise (Babar, 2024). Furthermore, business and technology users' concerns do not necessarily evolve as quickly as emerging threats, exposing them to increased security risks (Ahmadi, 2024; Aiken, 2016). Enhanced convenience also consistently threatens to undermine users' concerns for privacy by altering their cost/benefit calculus or simply nudging them into the ever-greater acceptance of privacy violations as a matter of course (Valasek, 2022).

The emergence of smart cities, for example, has produced significant challenges in this regard, and a key cloud business and data security priority consists of ensuring the privacy and security of all users' data even as the collection and transfer of data becomes an ever more ubiquitous feature of modern life (Habibzadeh et al., 2019). In short, from the cybersecurity standpoint, the privacy paradox must be considered regarding broader environmental and technological developments. Given the pressures on privacy in the modern digital environment, it makes sense that cloud business and data security professionals have turned attention to technological improvements to privacy, such as utilizing blockchain technology (Kshetri, 2017). According to Snipes (2024), it is reasonable to assume that cloud business and data security users

will maintain similar levels of impulsivity over time, with little likelihood of a significant decrease. Therefore, cloud business and data security professionals may wish to build privacy protections into the cloud applications and digital technologies themselves and, thus, do not depend as heavily on the self-control and discipline of the users (Collier, 2023). The threats themselves are also becoming highly sophisticated, as one can see from the new privacy threats that are opened up through the emergence and proliferation of AI-powered chatbots and other digital technologies of that sort (Gupta et al., 2023). Dealing with digital threats by only motivating business and technology cloud users was too weak to be influenced by online gaming behavior during the pandemic (Ostendorf & Brand, 2022). More realistically, they noted, strategies such as security built into the hardware, losses associated with impulsive behavior and improved privacy protection at the root level could help mitigate the risks.. Organizations must strategize cloud businesses to help mitigate the organizational privacy paradox by ensuring that business privacy safeguards are embedded directly into the technological infrastructure (Suntwal et al., 2025). Autonomous vehicles provide another example of a case where protections for privacy may need to be built in instead of relying on user compliance with best practices (Taeihagh & Lim, 2019). At least some of the literature on organizational cloud business and data security downplayed the importance of impulsiveness as such and instead called attention to the ways that cloud business and data security professionals can circumvent concerns regarding user impulsiveness when working to protect privacy (Gillam & Foster, 2020; Edwards et al., 2021; Diotaiuti et al., 2022). This approach may become increasingly important as the relevant technologies and threats become more complex, presenting a threat to privacy that could potentially dwarf the role of impulsiveness.

Nevertheless, Kannelønning and Katsikas (2023) clarified that human beings remain a weak link in cybersecurity efforts. Therefore, a subset of cybersecurity professionals must consider human factors when developing tools and systems to protect users' privacy. According to Al-Nuaimi (2024), several distinct behavioral and socio-cognitive factors influence people's privacy-related factors. Although this article does not pinpoint the impulsivity factor, its general findings are congruent with the points regarding impulsivity made in the previous section of this literature review. Likewise, Kont (2023) found that human factors play a significant role in cloud business and data security, with knowledge of potential risks being one important factor in this regard.

Overall, cloud business and data security professionals need to work toward building material security into digital technologies and information systems and help raise general awareness among users regarding threats to privacy and the importance of vigilance (Stewart, 2020). Starks (2022) contends that cloud business and data security professionals can become knowledgeable in the privacy threats and develop systems that objectively block off possibilities for human factors, such as impulsivity, to compromise users' privacy. However, the human factor will always be a weak link in cybersecurity efforts. Suppose people are careless about sharing their private information on the cloud. Ultimately, bad actors will find a way to take advantage of the situation and pursue their nefarious self-interest (Le, 2019). An awareness of human factors was thus important both for designing systems with those factors in mind and raising awareness about potential privacy threats (Ana, 2024). In this context, Sadeghi et al. (2023) suggested that cloud and data security business and technology professionals should be trained to reflect on their ethical priorities, given that such priorities often produce cybersecurity vulnerabilities. For example, people who prioritize speed, ease, and short-term gains may make ethical choices that

enhance the risk of cybersecurity vulnerabilities. Likewise, Pawlicka et al. (2022) suggested that the development of cybersecurity policies should be human-centered, which means that it should always be rooted in the awareness that cybersecurity professionals, end users, and bad actors are all human beings. Incentive structures, ethical decision structures, tradeoffs between values, and related matters will thus always be important when considering how best to protect privacy on the Cloud and within digital technologies and information systems.

Personality factors influence aptitudes and risks in this regard, as people with different personalities often have different degrees of awareness and risk tolerance (Anastasiei et al., 2020). Understanding how individuals interact with cloud technology and recognizing the inherent risks in their usage patterns, there is a need for cloud business and data security professionals to receive training not only in technical expertise but also in essential human and soft skills, which are crucial for developing effective security strategies and fostering responsible cloud utilization (Collier, 2023). Similarly, cloud business professionals also require self-awareness so they can recognize their risk factors and potential blind spots in relation to their threats and translate threats to systems (Sichel, 2021).

Summary. In this literature review section, I explored the theme of impulsivity and concern for privacy, as antecedents of human behaviors in cloud business and data security roles, and addressed the sub-themes of 1) Impulsivity and concern for privacy in security practices and 2) Impulsivity, personal information privacy, and personal factors in cloud business and data security management. The main idea throughout this discussion consisted of the privacy paradox, which refers to the phenomenon of people claiming to care about privacy but then engaging in individual behaviors under cloud business and data security settings that undermine privacy. Impulsivity was one of the main drivers of the privacy paradox. More broadly, human factors

produce cloud business and data security and cybersecurity vulnerabilities, such as insider threats, and professionals need to develop objective, material protections of privacy as well as more subjective features and interventions that take the irreducible human element into account, including the tendency of people to behave impulsively while managing cloud applications.

Impulsivity, Personality, and Individual Behavior Relationships

This section of the literature review explored the theme of impulsivity, personality, and human behavior, focusing on two categories: (1) the relationship between impulsivity and personality and (2) the connection between impulsivity and poor behavioral controls. A key finding examined in this discussion was the close relationship between impulsivity and personality traits, particularly the influence of openness to experience on the motor impulsivity domain. Personality-informed discussion revealed how personality influenced impulsivity and the ripple effect on human behavior through the lens of cloud business and technology, only to emphasize the inhibited behavioral control. Poor behavioral controls, in general, are highlighted as a potential risk factor that could undermine cloud business and data security practices, specifically, underscoring the broader implications of these dynamics within the cybersecurity landscape.

Impulsivity and Personality

The literature on impulsivity and personality made it clear that a connection existed between these concepts, even if they may sometimes be limited. Buelow and Cayton (2020), for example, conducted research on the relationships between three of the Big Five personality factors (openness, agreeableness, and extraversion) and performance on risky decision-making tasks. They found limited correlations between several factors (professional knowledge and social and engineering experience) and task performance. In another study, Indrajaya (2022)

found that people with high personality factors of openness to experience were more likely to engage in impulsive buying when engaging with online marketplaces and websites. This specific combination of factors could produce a temperament that found relief in letting go of behavioral control at times, in this case, through impulsive buying. In their study, Gratian et al. (2018) found that openness to experience was correlated with social engineering exploitations (curiosity, greed, deference to authority, and politeness), producing impulsivity interactions with the scammers and then impulsivity leading to software vulnerabilities, technical hacking, impersonations, and so on. This finding called attention to the fact that the openness personality trait was the most strongly value-coded out of the other personality factors (conscientiousness, extraversion, agreeableness, and neuroticism), which meant that being high in openness to experience was virtually always a negative personality descriptor that could be correlated with a range of behavioral problems. In Table 1 below, the scholarly work was presented within the last decade that was relevant to this research.

Table 1

Various Studies related to Impulsivity and Personality

Variable	Study
Work environment.	Ruth (2015).
Internet addiction.	Havrilko (2016).
Attitudes toward money.	Fenton-O'Creevy and Furnham (2019).
Cloud use disorder and social anxiety.	Peterka-Bonetta et al. (2019).
Performance on risky decision tasks.	Buelow and Cayton (2020).
Ethical attitudes.	Lee et al. (2020).
Emotional regulation difficulties.	Horwood and Anglim (2021).

Variable	Study
Consumer negative emotions.	Shemeis et al. (2021).
Big Five personality traits themselves.	Rizki et al. (2022).
Impulsive buying.	Indrajaya (2022).
Driving behaviors.	Luo et al. (2023).
Perceived job stress.	Johnson (2024).

Note. No focused studies found on individuals' dynamic personalities, impulsivity, and behavior.

Miglin et al. (2019) suggest that there may be a natural foundation for linking impulsivity with certain personality traits. Similarly, Horwood and Anglim (2021) identified emotional regulation difficulties as a significant factor contributing to problematic individual behaviors. Importantly, Horwood and Anglim (2021) demonstrated that the association with impulsivity was stronger than that attributable to personality traits per se. underscored how variables may be highly related to the personality factors without actually being derived from them. Evidently, a meaningful connection existed between impulsivity and personality; however, this relationship unfolded within the broader context of a complex array of personality-associated variables. The intricate interplay among these variables often complicates efforts to delineate the specific connections between them, with a comprehensive body of work that is carried out investigating relative variables to draw correlations to human behaviors, more connected explicitly to impulsivity and personality (see Table 1 above). Shemeis et al. (2021) examined the Big Five personality traits and their relationship with impulsive buying, finding that several traits were significantly associated with this behavior. Specifically, they identified consumer negative emotions as a full mediator in the relationship between openness to experience and compulsive buying. This suggested an additional variable related to impulsivity and personality traits, but it

cannot be reduced solely. Similarly, Rizki et al. (2022) reported that consumers' Big Five traits, such as agreeableness, openness to experience, and extraversion, significantly affected their impulsive buying behavior, indicating a positive link between Big Five personality traits and impulsive behavior. Simple as it is, the present study did not explore several variables that could have provided more insight into the relationship at hand. It is entirely plausible that, if tested, mediators and moderators would lead us to more complex relations between impulsivity and personality characteristics. The majority of other research in this area has demonstrated more etiologically complex relationships between impulsivity and personality attributes.

For instance, Fenton-O'Creevy and Furnham (2019) examined the relationship between personality and impulse buying, concluding that attitudes toward money were an important facet besides personality traits when shaping impulsive buying behaviors. This result was consistent with a complexity often noted in the literature, where the whole range of behavior/impulse behavior cannot be analyzed independently but within a more complex relationship involving other variables such as emotional and attitude components (Shemeis et al., 2021). Several empirical investigations (Evans, 2018; Serpico, 2020; Ryan, 2024) have investigated a variety of behaviors linked to impulsivity and personality characteristics, revealing their multifaceted nature. Similarly, Peterka-Bonetta et al. (2019) examined the relationship between smartphone and cloud use disorder and personality traits, uncovering the role played by impulsivity, social anxiety, and personality characteristics. These findings underscore the expanding interaction of factors that determine impulsive behaviors. Lee et al. (2020) reported that character traits and impulsivity were associated with academic dishonesty, suggesting a possible association with ethical attitudes. Furthermore, Luo et al. (2023) highlighted important relationships by trait of the driver, impulsivity, and specific driving behaviors. These studies (Lee et al, 2020; Luo et al.,

2023) collectively indicated that although a robust association was observed between impulsivity and personality traits, it was multidimensional and moderated by a variety of mediators, moderators, antecedents, and consequences.

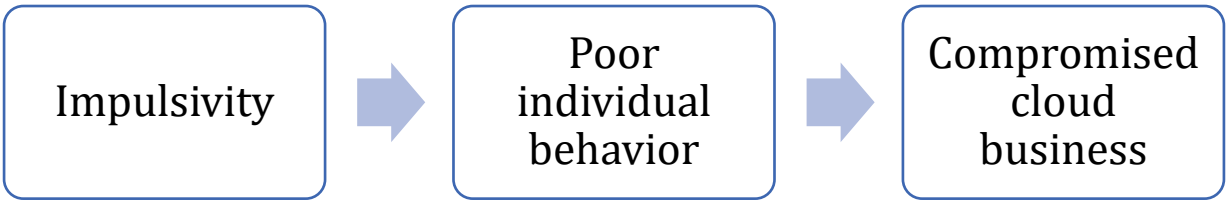
Impulsivity and Poor Behavior Controls

The focus of the theme of the literature review about impulsivity connected to the individual's behavior is rationalized by analyzing the association between the degree to which personality differences impact impulsiveness, which, in turn, reflects on behavioral consequences in different situations, and the cloud-based business and technology. Moreover, the study highlighted the importance of behavioral self-control in reducing impulsivity in cloud computing and data security domains. Poor behavioral regulation is a significant risk factor that can compromise security protocols and decision-making, thereby increasing vulnerabilities in cloud-based systems and leading to insider threats. Despite growing awareness of cybersecurity threats, cloud businesses, and data strategies primarily focused on technical solutions, such as encryption and multi-factor authentication, the behavioral dimensions of security management were neglected (Hwang, 2024). To delve into the relationship between impulsivity and compromised cloud business and data security environments, it will be appropriate to consider the relationship between impulsivity and poor individual behavior (see Figure 2 below). Organizational cloud business and data security depend on people being vigilant and in control of themselves with respect to sharing personal information, which means that poor individual behavioral controls will almost necessarily degrade cloud business and data security (Yahya, 2017). The literature on impulsivity and poor behavior was quite substantial in this context. Dezhkam et al. (2022) found that personality and impulsivity play a role in catalyzing perceived influence and addictive tendencies. For this study, impulsivity can be treated as a form of poor

behavior. Individuals who experience impulsiveness are likely to exhibit poor individual behavioral controls, such as addiction, decreased attention and planning ability, and increased motor activity, which can lead to compromised cloud business and data security. Similarly, Kun et al. (2021) examined the relationship between impulsivity and work addiction, finding that impulsive factors (motor impulsivity, attentional impulsivity, and non-planning impulsivity) were linked to poor behavioral controls.

Figure 2

Relationship between Impulsivity and Compromised Cloud Business



Note. Motor impulsivity compromised individual behavior in cloud business.

In a related study, Rachubinska et al. (2021) explored the connection between motor impulsivity and decreased attention to cloud policy controls, once again finding a significant relationship between these variables. The personality traits were highly linked to impulsivity, which in turn may lead to a deteriorating pattern of behavior and thus may affect cloud business and data security (Kiire et al., 2020). Malesza (2020) found that it was not unusual among dark triad individuals to present cognitive biases that may distort their reality perception. Melissa (2020) further illustrated that these biases may involve excessive faith in oneself and reduced belief in others' social relevance. Within this framework, it was reasonable to presume that dark triad people may struggle to evaluate information security threats or comprehend the implications of their decisions and actions (Wackler, 2021). As a result, personality traits were

closely connected to evil actions, and the dark triad personalities were also linked to weak behaviors, which further hamper cloud security resources in maintaining strong cloud business and data security (Zhang et al., 2023). Taken together, these findings highlight the importance of accounting for personality when examining security-related behavior, particularly in contexts like cloud business and data security management, and the literature suggested that personality traits are directly linked with impulsivity (Wackler, 2021).

Summary. Poor behaviors were not limited to impulsivity and included dysregulations of affect and cognitive biases to threats (Yahya, 2017). However, impulsivity remains strongly associated with weak behavioral controls, so personality characteristics related to impulsivity may be associated with weak behavioral controls (Rousseau, 2024). For example, Demircioglu and Kose (2022) examined the role of socio-demographics, the dark triad, and impulsivity in social-mediated dating. They found that people scoring the dark triad demonstrated greater impulsivity in using social media to find dating partners, increasing the possibility of disclosing personal information.

Moreover, though not examined in the current study, it might be reasonably expected that dark triad persons would be more likely to have others manipulate cloud-using participants to disclose confidential information, thereby damaging information security. Park et al. (2021) also discovered associations between impulsivity and self-destructive actions, highlighting that personality traits linked to impulse seek reward mechanisms can disrupt cloud business and data security controls, such as physical and online security. Although impulsivity has been acknowledged as a poor behavior on an individual level, especially in decision tasks requiring careful reflection and foresight, cloud business strategies seem to overlook impulsivity as an important behavioral determinant (Kont, 2023). Additionally, Kont (2023) noted that cloud-

based concerns were at greater risk if they did not have specific plans for addressing impulsive behaviors such as data breaches, unauthorized access, or loss of data, access, and compromised compliance protocols.

Operationalization of the Study Variables

In the present study, the predictor variable was motor impulsivity, which was associated with individual behavior; personal information privacy was the mediating factor that influenced

Table 2

Operationalization of Study Variables

Concept	Dimensions	Study Variable	Indicator	Scale
Impulsiveness dimensions	Attention, Motor, and Nonplanning	Motor impulsivity (Predictor)	Self-rating scale to measure the frequency of the tendencies to act spontaneously	ABIS (Coutlee et al., 2014)
Behavioral dimensions	Knowledge, Attention, and Individual behavior	Individual behavior (Outcome)	Participant ratings on a questionnaire assessing vulnerability to the threats caused by individual behavior	HAIS-Q (Parsons et al., 2014)
Big Five personality traits	Openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism	Openness to experience (Moderator)	Self-report inventory to assess open and closed mindedness in adapting unconventional ideas in cloud business and data security	BFI-10 (Rammstedt & John, 2007)
Privacy paradox	Personal Information privacy, Unauthorized secondary use, Improper access, and Errors	Personal information privacy (Mediator)	Self-report inventory to assess information collection privacy concerns of business and technology individuals	CFIP (Smith et al., 1996)

Note. Each study variable was measured with separate instruments.

impulsivity's transformation into individuals' behavior. Moreover, openness facilitated the relation between motor impulsivity and individual behavior. Individual behavior emerged as the dependent variable, captured how impulsivity, privacy concerns, and openness collectively shaped security-related actions in cloud business and data security management. The operationalization of the variables in this study as illustrated in the Table 2 above ensured that their measurement and analysis were precise and aligned with the study's conceptual framework. Motor impulsivity, a key antecedent variable, was operationalized using the established Abbreviated Impulsiveness (ABIS) scale (Coutlee et al., 2014). This construct was treated as a quantifiable factor, grounded in self-report assessments and behavioral observation metrics. Individual behavioral outcomes in cloud business and data security are operationalized as dependent variables and are measured through the Human Aspects of Information Security (HAIS) survey scale (Parsons et al., 2014).

Similarly, personal information privacy was operationalized as a mediating variable through the Concern for Information Privacy (CFIP) survey scale (Smith et al., 1996). These instruments provide empirically valid and reliable data to evaluate privacy concerns as a mediating factor. Openness to Experience was treated as a moderating variable. However, it was measured with proven scales like the Big Five Inventory (BFI) that evaluated the extent of participant openness, creativity, and willingness for experience with the scale BFI-10 (Rammstedt & John, 2007). These operational definitions in Table 2 above together form an organized procedure of analyzing the connection between mortalities and the study variables in general; at the same time, they need to be in accordance with the main conceptual model of the study.

Summary. This part of the literature review focused on impulsivity, personality, and human behavior in organizational cloud business and cloud data security, with an emphasis on two main sub-themes: (1) impulsivity, personality, and human behavior, and (2) impulsivity and individual behaviors in cloud business and data security. I also introduced motor impulsivity, personal information privacy, openness to experience, and individual behavior as constructs, allowing the examination of their interdependence between cloud business and data security management. To enlighten the logic of the concept in this issue, it should be mentioned that it would be problematic if the personality traits were directly related to impulsivity, because personality traits were not intended inherently to dictate specific behaviors that could influence security and business risks. One of the behavioral dimensions, impulsivity, was a relevant factor that had a crucial impact on this relationship, as underlined in the current research. Effective behavior management played a critical role in ensuring secure information systems because individuals with weak behavior management were easily influenced and had become weak links in information systems (Evans, 2018).

One of the findings that emerged was the confirmation of impulsivity as a dimension of personality that formed in relation to a complex net of variables. In summary, it was important to let out the complex interaction between impulsivity and personality, to enable intervention for behavior vulnerabilities in the cloud business and data security. This point was also reminded by the highlighted dynamics of poor individual behavior as a mechanism of impulsivity, where the strong behavioral control was needed in order to reduce the business and security risk (Rizki et al., 2022). Enhancing these controls was necessary to protect information systems and minimize the risks of those employees with lower levels of behavioral control.

Conclusion

This chapter revealed the complex interrelationship of impulsivity, personality, and human behavior against organizational cloud security. Research consistently showed that it was not an isolated quality but tended to be highly correlated with other personality traits, such as tendencies toward risk-taking (Rachubinska et al., 2021). Studies like Hadlington (2017) and Aivazpour & Rao (2022) have highlighted that impulsive people often tend to show behavior that could result in higher risks of cloud business and data protection risks (which may not always be straightforward) or produce irrational decision-making (at least in office settings). In addition, this chapter revealed the moderating effects of personality factors, which helped to explain the mechanism of impulsivity towards distinctive privacy protection behaviors in cloud business and data security management.

In particular, the partial mediation of personal information privacy demonstrated that the privacy concern does not consistently operate as a direct determinant but can be mediated through impulsivity, which counters traditional theories that suggest privacy concerns are directly linked to security behaviors. Instead, the evidence indicates a more situational model, in which impulsivity interacts with individual dispositions, workplace security regulations, and the broader culture of the organization to influence decisions, which will be done in the next chapter, presenting a comprehensive account of the methods involved in the study, a study that is a precursor to quantitative research and aimed at testing the construct in this study.

Chapter 3: Methodology

This section entailed a discussion of the research design and methodology for the completed study. Parts of the chapter include a description of the research participants, the operationalization of variables, a discussion of reliability and validity, and measurement and instrumentation. Other subsections include the plan for data collection and collection procedures, as well as the data analysis procedures for the study.

Description of Research Participants

The research participants for this completed study were drawn from the cloud security and data management workforce, a demographic that has expanded significantly in recent years. Following the COVID-19 pandemic, the prevalence of cloud business and data security management, remote business operations, and mobile application access surged dramatically. While only 15% of professionals engaged in remote business activities during the 2018–2019 tenure, this figure increased to 87% by 2021 (Office of the National Coordinator for Health Information Technology, 2023). Among these virtual workforce, IT professionals and insurance agents were the most frequent users, accounting for 96%, followed closely by accountable care organizations (ACOs) operating under public or private insurance arrangements, at 94% (Office of the National Coordinator for Health Information Technology, 2023). The general population of virtual users in the United States, who served as the foundation for this study, represented 9,043,070 workforce members in 2022 (Bureau of Labor Statistics, 2023). This quantitative study specifically targeted business and technology professionals operating in cloud business and data security environments to evaluate their vulnerability to insider threats. The focus was on assessing how motor impulsivity influenced their behaviors in cloud business and data security business management, providing critical insights into the human factors contributing to business

and data security risks in digital environments. The study focused on individuals working within the field of cloud business and data security management. Rather than targeting general cloud application users or other cloud data consumers, the study concentrated on cloud business and data security professionals working in financial organizations investing in cloud transformations for over a decade. This focus stemmed from the personal work experience that the security behaviors of cloud business and data security professionals were closely linked to insider threats in addition to multiple future research suggestions, a concern heightened by the increasing adoption of hybrid work environments and the frequent transfer of data across misconfigured digital storage systems (Meinert et al., 2018; Cremer et al., 2022; Nifakos et al., 2024; Aschwanden et al., 2024;). The study population included business and technology executives, managers, architects, analysts, and engineers.

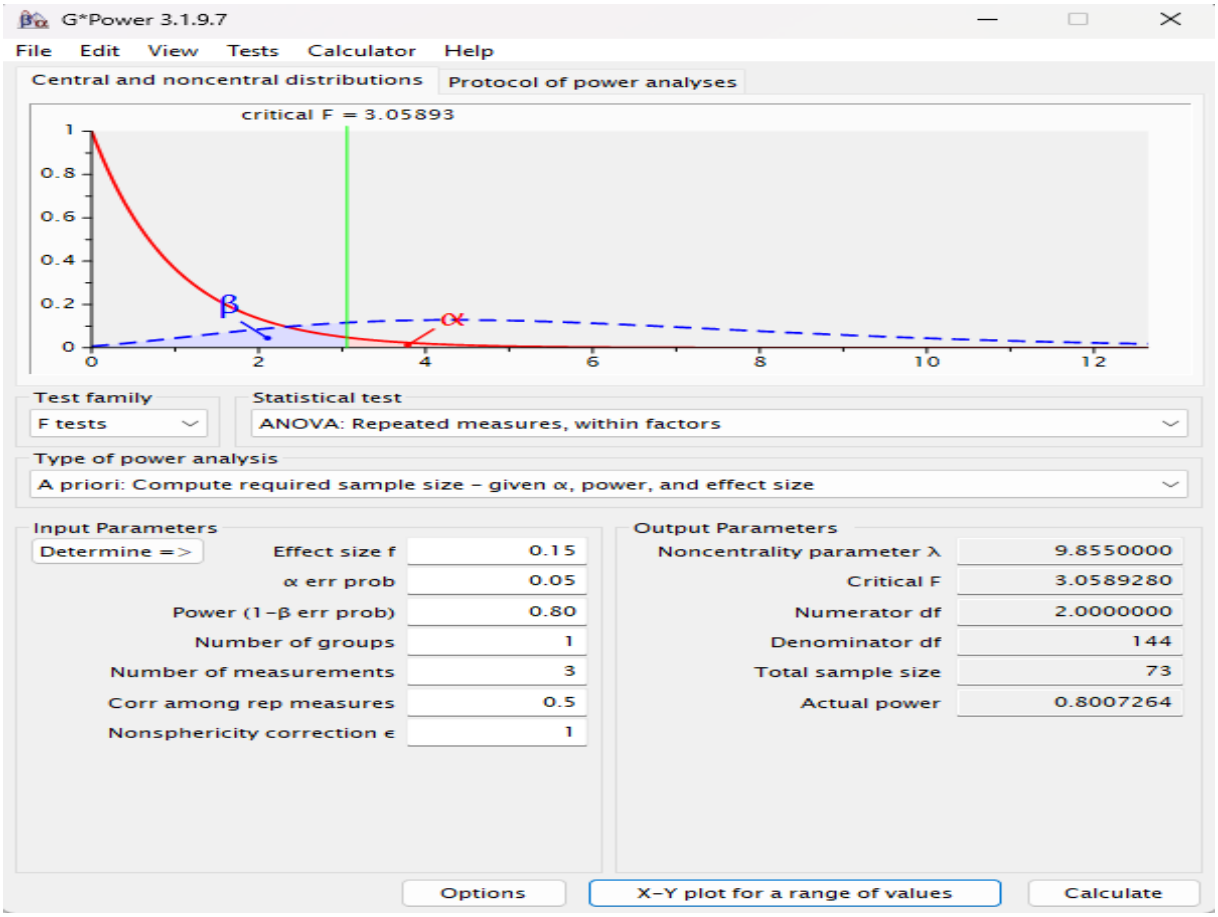
Sampling Strategy and Sample Size

Purposive sampling, often called judgmental, selective, or subjective sampling, is a nonprobability sampling method characterized by selecting specific participants based on certain predetermined criteria (Palinkas et al., 2015). The goal of purposive sampling was to target specific population characteristics relevant to the study, enabling the researcher to effectively address the research questions (Durodolu, 2016). In the context of the research questions, which address the interplay between personality characteristics, impulsivity, and individual behavior in cloud business and data security business and technology, the sampling strategy were keenly attentive to specific groups. The sample for the present study was estimated through an a priori power analysis. Using G*Power software version 3.1.9.7 (Faul et al., 2009), a power analysis was conducted to determine the required sample size for the study was calculated based on “A Priori” type of power analysis using G*Power (Faul et al., 2009). The power analysis results in

Figure 3 exhibited that the input parameters included a medium effect size of $f^2 = 0.15$, an $\alpha = 0.05$, a power of $1-\beta = 0.80$ was set with an indication to reject null hypothesis at 80% probability rate, and three predictors. The results in Figure 3 also indicated a noncentrality parameter λ of 9.85 and a critical $F(2,144) = 3.1$. with a sample size of $n = 73$ achieving a power of 80.07%.

Figure 3

A Priori Power Analysis



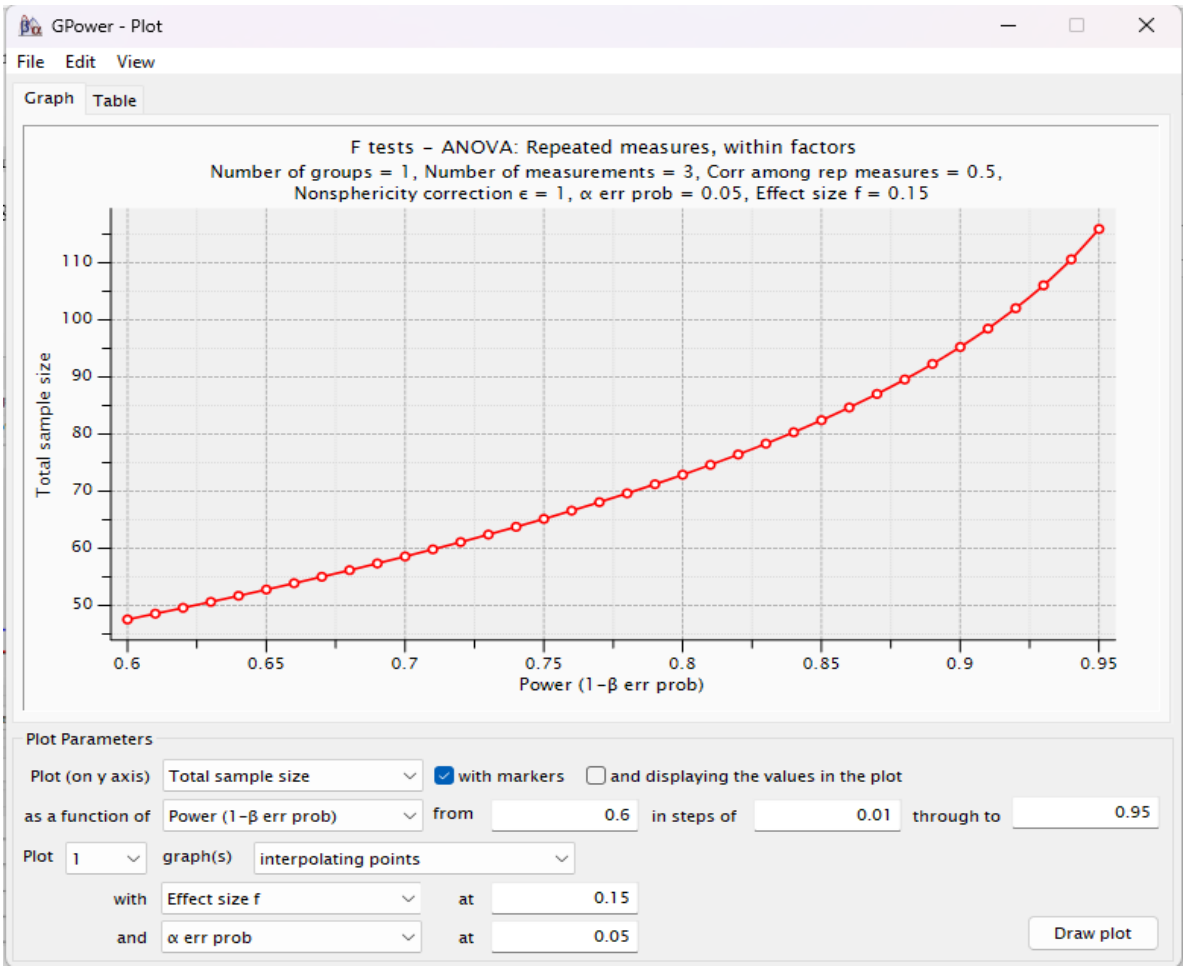
Note. Required sample size n=73 was achieved for power of .8.

From Figure 4 below, it was revealed that the statistical power from .6 to .95 on the x-axis and the required sample size on the y-axis confirmed that the total sample size was 54 to achieve

80% power, and about 74 total sample size was needed to achieve 90% power. Since 150 total sample size was employed in this study, it can be concluded that the design was efficient.

Figure 4

GPower Plot Window



Note. Approximately total sample size of 74 achieved 90% power.

While this analysis determined that a minimum sample size of 73 was statistically sufficient, the researcher contracted with Qualtrics to obtain 150 participants to enhance the robustness and reliability of the study's findings. A sample size of 150 offered several advantages over the minimum requirement. One part of the reason for sample size effects is increased statistical power due to larger sample size, which in turn reduces Type II error (i.e., a failure to find a true

effect when it actually exists). Second, it resulted in a more diverse dataset, which offers more generalizability in the cloud business and data security community. Third a sample size supported sufficient precise estimated effect sizes and allowed to explore subgroup analyses that expanded understanding of the relationships among the study variables.

Reliability and Validity

Reliability and validity were critical characteristics of research because they support the fidelity of the research. To ensure reliability and validity, the researcher utilized well-established measurement instruments rigorously tested in prior studies (de Paula et al., 2020; McCormac et al., 2017; Stewart & Segars, 2002; Xu et al., 2023). The HAIS-Q (Parsons et al., 2014) assessed individual behavior, ensuring consistency in measuring cybersecurity awareness and related actions. Motor impulsivity, the independent variable, was assessed via the ABIS (Coutlee et al., 2014), which was a validated measure known for its reliability in assessing impulsive tendencies. The CFIP (Smith et al., 1996) was used to gauge personal information privacy, a widely recognized scale for evaluating privacy concerns and attitudes. Additionally, openness to experience, the moderator variable, was assessed using the BFI-10 (Rammstedt & John, 2007), a reliable shortened version of the Big Five personality inventory. These instruments were chosen for their strong statistical measurement properties, ensuring that the collected data was consistent (reliable) and representative of the measured constructs (valid). Using well-established scales, the process can guarantee the methodological rigor, contribute to the credibility and feasibility of the conclusion of individual behavior in cloud business and data security research.

The researcher ensured reliability in the study by delivering the survey instrument to all participants in a similar manner (Ahmad et al., 2019). A digital survey was designed to collect data to ensure consistency in data collection. The researcher tested internal consistency after data

collection. Internal consistency was assessed based on Cronbach's α. An $\alpha \geq 0.70$ will be considered acceptable. Additionally, convergent validity was assessed in SPSS using Pearson's r to determine whether the study constructs designed to measure the same concept or phenomenon were positively correlated.

Instrument Development

Parsons et al. (2014) amplified the Human Aspects of Information Security (HAIS-Q) questionnaire to measure information security KAB tailored for the organizational business and technology environment. Information security understanding was pivotal in protecting enterprises from data breaches and cyber threats (Senyo et al., 2019). HAIS-Q was tested on diverse samples, and the validity of a 63-item questionnaire as an effective instrument to measure information security awareness was evaluated in two studies (Parsons et al., 2017). Parsons et al. (2015) applied the HAIS-Q to explore the relationship between organizational culture and information security awareness and further reported Cronbach's alphas of above .80. McCormac et al. (2017) recently reported Cronbach's alphas of above .80 during the investigation of personality, gender, and age association with HAIS-Q scores. Because the focus areas of the HAIS-Q cover aspects like password management, incident reporting, cloud use, etc., that are relevant to the current study, the questionnaire items (21) were adopted, and the validity was assessed based on the results of tests for convergent and discriminant validity in prior research (Pattinson et al., 2015).

The current study involved a shortened Abbreviated Barratt Impulsiveness Scale (ABIS), a 13-item impulsivity scale developed by Coutlee et al. (2014), to avoid any response fatigue from respondents. Without losing the Barratt Impulsiveness Scale 11 (BIS-11) construct's validity, the researchers condensed 30 items to 13-item questionnaires to improve the reliability

of measuring impulsivity. The ABIS consisted of three subscales, such as attention, motor, and nonplanning, and each of these reported Cronbach's α of 0.80, 0.82, and 0.71, respectively (Coutlee et al. (2014). According to Rammstedt and John (2007), using shorter personality-type instruments was accelerating as researchers need more assessment tenure. Rammstedt and John (2007) further supported development and evaluation of five and 10-item Big Five instrument (BFI), which benefited cloud-based studies with a high average validity compared to Big Five 44-item inventory. Chang et al. (2017) pointed out that long inventories will lose participants' attention; more specifically, technological longitudinal studies with single-item brief instruments will avoid item redundancy and help answer similar questions repetitively. Thus, the researcher adopted Rammstedt and John's (2007) BFI-10 as the instrument in this study, which was feasible and predicts suitable personality traits.

The CFIP instrument, developed by Smith et al, (1996), was a four-dimensional instrument that included personal information, collection, errors, and unauthorized access. Chang et al. (2017) used CFIP to investigate social networking privacy concerns. Bélanger and Crossler (2011) used the CFIP instrument and yielded discriminant validity in a mobile technology adoption study to examine the effect of unauthorized access mediation. Furthermore, Dogruel et al. (2017) explored errors, collection, and personal information using a 15-item inventory, revealing that each dimension was reliable and distinct on the CFIP scale. The current study adopted Chang et al.'s (2017) CFIP nine-item inventories to measure one of the domains, personal information. Overall, the researcher employed a 39-item survey questionnaire including demographic information to score on a five-point Likert scale and allow participants to self-report the responses on Qualtrics survey platform.

Measurement and Instrumentation

Instrumentation for the proposed study involved using a survey on the Qualtrics digital survey platform. Qualtrics, the world's leading enterprise survey technology solution and XM platform supplies quality samples from traditional and actively managed research panels (Sürücü & Maslakci, 2020). Qualtrics Panel, a sub-division of Qualtrics, specialized in academic research and survey-based data collection to supply diverse and quality respondents. The Qualtrics project team screened study respondents to determine eligibility by providing a six-question screener on their web survey platform. Eligible participants received an email informing them about the length of the survey, that the study was for research purposes only, and what incentives were available. Respondents received an incentive, and the specific rewards included airline miles, gift cards, redeemable points, charitable donations, sweepstakes entrance, and vouchers. Participants were allowed to unsubscribe at any time. The Qualtrics project team ensured that survey invitations were generic and did not include specific details about the contents of the survey to avoid any self-selection bias.

The informed consent form was provided and signed. The consent form provided an overview of the study purpose outlined participants' responsibilities, including what was required of them during the study, as well as instructions on how to withdraw from the survey if they choose to do so. The third page consisted of demographic questions and selected items from established scales to measure the study variables. The measurement items from the ABIS (Coutlee et al., 2014), BFI-10 (Rammstedt & John, 2007), CFIP (Smith et al., 1996), and HAIS-Q (Parsons et al., 2014) scales were included in Qualtrics survey questionnaire. Participants were selected based on specific criteria, including employment within the United States, who worked in business and technology environments, affiliated with cloud transformations that supported

digital business operations, and formal or informal practice of cloud data security. A Likert scale format was utilized for survey item development, combining various scale items to assess the study's key variables systematically. This approach ensured accurate and reliable data collection to explore the relationships central to the research.

Data Collection Plan and Procedures

The research documentation about the data access, informed consent, and data security was reviewed and received full approval from the Franklin University Institutional Review Board (IRB) to comply with human subject protections. As part of the review process, the study was diligently assessed for its risk and ethical considerations. After a thorough review, the study was deemed exempt from IRB approval (i.e., the study presented no greater-than-minimal risk and involved no procedures that could harm the subjects). The exempt design (since the design of this study only included survey-based data collection), which meant no invasive interventions, sensitive and/or aggravating tests that would be used to collect data. Control, manipulations, and high-risk items. This categorization indicates that the participants did not experience undue distress, risk of breach of privacy, or ethical issues. Matching typical literature practices with self-reported data. The process of obtaining IRB approval also reminded the researcher about how important it is to keep confidentiality, obtain informed consent, and ensure that participation is voluntary. The purpose of study, process, and the rights of the participants were explained to all the subjects, thereby ensuring transparency throughout the process. The study was consistent with federal and institutional ethical guidelines and obtained IRB approval as exempt, that is, did so in a way that did not jeopardize the well-being of participants and was designed to allow for responsible academic inquiry. The information on IRB approval appeared in Appendix A, which outlined the purpose, decision status, and research notes.

After obtaining IRB approval, the researcher worked with the Qualtrics project team to create and program the survey in a way that would enable the collection of data that was organized to meet the purpose of the study yet provide some level of anonymity to those completing the survey. The team developed a confidential, anonymous distribution link for the online survey participants during this preparation. Then, the Qualtrics project manager thoroughly reviewed the survey's overall configuration, functionality, layout, and user experience to ensure the instrument functioned properly. The screener logic screen was incorporated in the survey flow to screen potential participants according to the predetermined eligibility criteria specified in this study, as it was necessary to ensure the quality and relevance of the collected data to the research questions. Once the survey was set up, the project team began with a soft launch, a first step towards launching, in which the survey was tested on a manageable scale before being distributed to the entire audience. This pilot phase revealed any technical glitches, inconsistencies, or respondent issues that allowed us to make the necessary refinements before final deployment.

The researcher also served an important verification function by carefully reviewing the survey programming, demographic filters, and question logic for accuracy and correlation to the study design. Finally, confirmation of data integrity validated system components—such as order of questioning, language used, and logic to capture information for the most clarity and precision—mitigating potential for bias or respondent bewilderment. These meticulous preparations ensured the survey's trustworthiness and validity, which helped ensure that high-quality data could be obtained for meaningful analysis.. The Qualtrics platform also facilitated the entry of survey responses and provided a user-friendly interface for participants to engage with the survey items. The survey itself included multiple components: the inclusion and

exclusion criteria, the informed consent form, demographic questions, and items from four established scales, including ABIS (Coutlee et al., 2014), HAIS-Q (Parsons et al., 2014), CFIP (Smith et al, 1996), and BFI-10 (Rammstedt & John, 2007). The inclusion and exclusion criteria were outlined on the first page of the survey, specifying that participants must have at least 7 years of professional experience in cloud business and data security management. Prospective participants needed to be in roles with job responsibilities that included data security management, operations, technical support, cloud data management, and security. To the extent that a participant failed to meet these criteria, the Qualtrics team informed the researcher of the participant's ineligibility and removed them from the survey. It resulted in the training of motivated workers who were ready to organize. Participants were added, preserving the validity and reliability of the obtained data. This systematic approach ensured the integrity of the sample and the reliability of the data collected for the study (Sürücü & Maslakci, 2020).

The Qualtrics survey invitations for this study were straightforward and designed to encourage participation without introducing self-selection bias. Each invitation included a hyperlink directing respondents to the survey and outlining the incentives offered. Participants were informed of their ability to unsubscribe at any time. Additionally, some respondents encountered surveys they likely qualified for upon signing into the panel portal. The invitations were purposefully nonspecific and did not explicitly describe the survey content to avoid biasing participation. Participants were asked to complete the brief questionnaire after meeting the inclusion criteria. The second page included the consent form requiring a digital signature's remission before access was allowed. The third page provided directions and the survey items. The researcher actively monitored data collection until the minimum sample size was achieved. Qualtrics automatically replaced any respondents who completed the survey in less than half the

median completion time. Within seven days of survey completion, the researcher thoroughly reviewed the results and collaborated with the Qualtrics team to address any quality issues, ensuring that only valid responses were included in the final analysis. The details of informed consent and survey questions were exhibited in Appendix B.

Data Analysis Procedures

After data collection, the researcher downloaded the data set from the Qualtrics to Microsoft excel (version 2023) for preliminary analysis and examination. This consisted of data cleaning, data organization and data clean-up interventions for further analysis. The researcher scanned the data set for missing and questionable records. If the missing value was random, in compliance with Kang (2013) the whole data point was excluded. However, this approach was only applied when the remaining observations were sufficient to ensure reliable analysis. The review process also considered the three primary sources of missing data highlighted by Ali et al. (2018): item nonresponse, noncoverage, and total nonresponse. Weighting techniques could not address data missing due to nonresponse.

However, Palinkas et al's. (2015) approach to address missing data was employed to check if the reduced sample size still adequately represented the target population. This careful approach ensured the quality and integrity of the data prepared for analysis while maintaining its relevance to the study's objectives. For instance, if data on the variable Y (age) is missing completely at random (MCAR), the absence of this data is entirely unrelated to the predictor of motor impulsivity within the dataset (Al-Nuaimi, 2024). Additionally, there were no patterns in which respondents from either high or low age groups systematically failed to respond, ensuring that the missing values occurred independently of observed and unobserved data characteristics.

The researcher analyzed MCAR data as if working with the entire sample, ensured generalizability remained intact and no such situation was observed to remove cases from the dataset. Fraudulent data where the same responses were selected or where there were ascending or descending patterns were not found to remove from the dataset. Metadata such as I.P. addresses, dates, times, I.D. hash data, etc., given by Qualtrics for individual cases were removed from the dataset. Qualtrics (2025) implemented the following data protection and data security measures:

> Qualtrics' database does not hold sensitive or confidential panelist information; however, we do hold all survey responses in our data centers. Our data centers utilize many security measures. Qualtrics' database access is restricted and requires authorization. All computer equipment (servers, SANs, switches, routers, etc.) is redundant and is located in secure, environmentally controlled data centers with 24/7 monitoring. Web traffic does not directly access the database and database requests are reversed proxy via an application server to the database. All information is secured via industry standard firewalls and stringent IT security policies and procedures. We utilize industry standard web application firewalls and DDOS protection. Qualtrics also leverages sample partners who are meticulous in their multiple levels of security that include redundant data centers, secure servers, encryption which includes one-way encryption, numeric IDs, secure .NET platforms, security clearance, industry standard firewalls, 24/7 monitoring of data centers, confidentiality agreements, and physical, electronic, and managerial procedures. (p. 7, #25)

After completing data collection, the researcher saved the data as a comma-separated values file and securely stored it on an encrypted USB drive. Data was reloaded at SAS Studio and SPSS

version 27.0.0.0 and also saved on the same encrypted USB drive. This drive included all the analysis files and will be maintained for at least 5 additional years. The researcher intends to wipe out all of the data, breaking the drive after 5 years, in order to maintain the security and ethical standards. The second step was to evaluate the credibility of the information. Internal consistency for each variable was assessed with Cronbach's α, and the criterion for acceptability was if $\alpha \geq 0.70$. Furthermore, boxplots were also used to check the presence of outliers in the dataset. Univariate outliers found through this process were excluded, whereas influential ones were retained and reported in order to prevent compromising the integrity of the analysis. This thorough procedure guarantees the quality of the dataset used in the study. Analysis for the finished study was conducted at four levels: cleaning, organization, and preparation of the data. Phase 1: In the initial phase of demographic analysis, the researcher studied the demographic profile of the respondent. Analyzed demographic variables included age range, gender identity, and race/ethnicity. These features were quantified as possible frequencies in percentages and counts in order to provide a straightforward description of the study population. The second phase of analysis involved calculating descriptive statistics for the variables of study. These descriptive statistics constituted central tendency measures (mean) as well as distribution measures (standard deviation).

Skewness and Kurtosis were also estimated to check the posterior distribution of the data. These analyses laid down the groundwork in order to be able to understand the characteristics of the dataset further and for the preparation of more sophisticated statistical analyses. During the final stage of the study, the third level of the data analysis was realized: statistical assumptions were tested. Statistical methods utilized for examining the study hypotheses involved bootstrapping for mediating effects and hierarchical regression for moderating relationships.

Moreover, statistical assumptions such as linearity, normality, and homoscedasticity were tested. The linearity test utilized scatterplots, with acceptance of linearity determined by identifying patterns between the top-right and bottom-left or the top-left and bottom-right. Normality was tested based on the residuals of the regression analysis, using the Shapiro-Wilk test. Results with $p < 0.05$ indicated a non-normal data distribution. Multicollinearity was assessed using the variance inflation factor (VIF), with VIF > 4.00 indicating the presence of multicollinearity. The Durbin-Watson test was applied to test autocorrelation, with values between 1.5 and 2.5 suggesting a lack of autocorrelation. Homoscedasticity was examined through scatterplots, with a random distribution indicating that homoscedasticity could be assumed.

Intellectual Merit

This thesis successfully explored the relationship between motor impulsivity, openness to experience, personal information privacy, and individual behavior, especially in cloud business and data security technology in remote operation, such as cloud business and data security companies. By utilizing the generalizable Big Five personality trait (openness to experience), the study developed a sound foundation to address critical research questions. The results highlighted the importance of the moderator effect of personality traits in the relation among impulsivity, the human factor, and security behavior, providing a better understanding of how individual human dispositions affect vigilant behaviors for cloud business/data security. This study also fills with research gaps regarding impulsivity in cloud business and data security. Moreover, the research also explored the mediation mechanism of personal information privacy, by revealing how personal data privacy concerns affect and reconstruct the binocular relationship between impulsivity and security, influencing individual behavior actions. The study yielded important and unique findings concerning the separate effects of personality and privacy

concerns and an overarching framework that linked them. This integrated approach laid down the groundwork for next-generation interdisciplinary studies, provided knowledge advancement in the area of human factors in cloud business and data security, and has the potential to make theoretical and practical contributions.

Broader Impact

Understanding the complex components of potential weaknesses in cloud businesses could make a big difference to data security in both high-end technology and start-ups. As the cloud business involves privacy technology, the data security business operation is paramount; laying the foundation for data security is the core of the digital enterprise. Unpacking the findings from this research could directly influence the creation of training programs. Instead of one-size-fits-all modules, cloud-based businesses could cultivate awareness campaigns and educational initiatives tailored to distinct personality profiles, drastically reducing the potential for human error and security breaches. On the policy front, as remote business platforms proliferate, there is a pressing need for adaptive regulations towards adopting web-based and mobile applications (Yamin & Alyoubi, 2020).

The insights from this research can inform policymakers, allowing them to craft regulations that seamlessly merge technological progress with the idiosyncrasies of human behavior. Beyond the tangible aspect of data protection, this research also resonates with the economic pulse of business entrepreneurship. By proactively addressing and minimizing the risk of security breaches, high-technology and business sectors can avoid the extreme costs associated with data compromises. Finally, the emphasis on privacy concerns in the research narrative magnifies the ethical dimension of data protection. It served as a reminder of the moral responsibilities that cybersecurity plans shoulder and emphasized the importance of maintaining

the sanctity of corporate applications and data. In essence, the research advanced academic discourse and contributed to various societal facets, from data security to individual behavior, economic implications, and ethical obligations.

Ethical Considerations

Several ethical considerations grounded in the Belmont Report were meticulously addressed in this completed study on the relationship between impulsivity, the Big Five personality characteristics, personal information privacy, and individual behavior in cloud business and data security management. The Belmont Report (U.S. Department of Health and Human Services, 2024) outlined three foundational ethical principles for research involving human subjects: respect for persons, beneficence, and justice. By embedding these principles into the research process, the study adhered to high ethical standards and safeguarded the welfare and rights of its participants. The principle of respect for persons, which mandated treating individuals as autonomous agents while providing additional protections to those with diminished autonomy, was carefully upheld.

To operationalize ethical principles, the digital survey administered to cloud business and data security included a comprehensive informed consent form accompanied by professionals. This document explicitly described the nature of the study, the procedures required, the risks and benefits, and stated that they could opt out of the study without any adverse effect. The study honored their autonomy and protected their informed participation by ensuring that participants fully understood the research's purpose and implications before consenting. The principle of beneficence insisted that the well-being of participants be at the forefront of the research's design and implementation, which involved doing no harm and maximizing potential benefits while minimizing potential risks. Given that the study involved a digital survey, one might assume

minimal risk. However, given the sensitive nature of personal and business privacy in the cloud business and data security domain, there was the potential for psychological discomfort or fear of professional repercussions. To uphold the principle of beneficence, the researcher worked with the Qualtrics project team to ensure survey responses were kept anonymous, without any identifiable personal or professional markers. Furthermore, data was securely stored and only accessible to the researcher, avoiding any breach of the participants' privacy. Justice, the third principle of the Belmont Report, demanded that the benefits and burdens of research be distributed fairly.

The chosen population for this study, cloud business and data security professionals, was not selected merely because of ease of access or manipulability, but because they were most pertinent to the research questions. Moreover, the researcher diligently avoided unintentional biases in survey distribution that might have excluded certain groups within the cloud business and data security community. Results were shared to help others in the broader community for cloud business, data security, and cybersecurity, to serve as more practical, tangible applications besides academics. It should be noted that no efforts were made to assess the real security mechanisms provided by the participants' cloud business and data security platforms. This method preserved the proprietary and confidential character of participants' platforms and ensured that their professional tools and practices were not being made the focus of investigation.

Incorporating the Belmont Report, respect for individuals, beneficence, and justice, the investigation fulfilled its ethical responsibilities scrupulously and meticulously. Additionally, I have addressed fair participant recruitment and no biased data interpretation to reduce ethical issues of representation and validity. Care was taken in the design of the sample selection so that

the sample was not biased and was as diverse as possible from the respondents. Furthermore, the researcher used objective techniques to reduce possible bias, and the findings were verified with the data. Institution Review Board (IRB) ethics proposals were requested and granted to underline the best ethical practice of conducting research (Franklin, 2025). See Appendix A for the IRB approved letter. This responsibility ensured the protection and safety of subjects, as well as the validity, credibility, and generalization power of the findings of this research in the setting of cloud business and data safety.

Chapter 4: Data Analysis Results

This chapter presented the findings of the quantitative study examining the relationship between human behavioral factors and cloud security management within digital enterprises. Specifically, the study examined how motor impulsivity influenced individual behavior and how its interaction with openness to experience and personal information privacy affected security-related individual actions in digital environments by cloud business and data security professionals.

The chapter was organized to clearly and systematically presented the study results with an overview of the participants' sample characteristics and demographic information in the beginning, which is followed by a description of the data preparation process, including data cleaning, normalization, and verification of statistical assumptions. Next, the chapter detailed the statistical methods employed, such as descriptive statistics, correlation analysis, and regression analysis, to study the relationships among the key variables: individual behavior, motor impulsivity, openness to experience, and personal information privacy. The results of these analyses were then presented and interpreted, highlighting the behavioral factors that significantly influenced cloud security practices within digital enterprises. Finally, the chapter concluded with a summary of the significant findings, setting the stage for the subsequent chapter, which discussed the broader implications, recommendations, and contributions of this study to understanding human decision-making and data security risks in digital enterprises.

Purpose

The drive of Chapter 4 was to report and discuss the data analysis about the research questions. Data analysis method and results were described, including data preparation, statistical hypothesis testing, and results. Furthermore, the relationships between the study variables such

as motor impulsivity (independent variable), openness to experience (moderator), personal information privacy (mediator), and individual behavior (outcome/dependent variable) were described while summarizing descriptive statistics, regression analyses, correlation tests, and any significant findings addressing the research questions in the light of cloud business and data security literature.

Overview of the Analysis Methods

This researcher used various statistical analyses to address the research questions, including RQ1: Does motor impulsivity impact individual behavior in cloud business and data security management? Moreover, RQ2: How does privacy of personal information mediate, and how does the Big Five personality trait of openness to experience moderate, the relationship between motor impulsivity and individual behavior in cloud business and data security management? The statistical analyses were conducted using SAS and SPSS software. The analysis began with demographic profiling, followed by descriptive statistics to provide an overview of the data measurement of central tendency (mean and median) and dispersion (standard deviation, range). Next, assumption testing was conducted to ensure the data met the normality, linearity, and homoscedasticity assumptions of the statistical tests.

The core analyses were conducted using the Shapiro-Wilk test, and the core analyses included a multiple regression model to illustrate the relationships between independent variables (e.g., motor impulsivity, openness to experience, and personal information privacy) and the dependent variable (individual behavior in cloud security). Finally, the hypothesis testing was performed to determine statistical significance (α) and further accept or reject the null hypotheses.

Data Collection, Preparation, and Results

Summary of Data Collection

Key business and technology staff with roles involved in cloud business and security technology were surveyed regarding how the technology aspects of the business operate and provide technical support to key departments, including cloud data management and data security. Of the 200 respondents who expressed interest in participating in the questionnaire, 30 individuals were deemed ineligible and excluded from the study. In summary, 170 questionnaires were completed for the survey, but 20 sheets were excluded from the final analysis due to incomplete data. The sample size after evaluation was 150 participants. The total sample size was in accordance with a priori power analysis (73 participants).

The questionnaire was designed to measure cultivable aspects of individual cloud security management behavior, including antecedents such as motor impulsivity, openness to experience, and privacy concerns regarding personal information. They were all offered the opportunity to complete a structured study survey, which took less than ten minutes to fill out. The investigator included a cross-section of cloud security practitioners in the sample to make it more representative of the overall population. Data Collection: The data were collected as part of a pre-existing survey, which included the survey questions of interest for this study. The wording of the survey questions was not altered; however, the response options were adjusted to capture nuanced observations relevant to this research. The 39-question survey covered a range of factors affecting cloud business and data security management practices. The brief time period was crucial in reducing respondent fatigue and maintaining a high response rate to attain responses for all 63 subscale items on the questionnaire.

Handling Missing Data

Out of the initial 170 participants, only 150 provided complete responses, and their data were selected for analysis. The exclusion of incomplete surveys did not significantly impact on the integrity of this study, as there was a sufficient sample of 150 to draw meaningful conclusions. By using strict data validation and maintaining an adequate sample size, the reliability and generalizability of the findings in this study were not compromised. Therefore, it is unlikely that the missing data will influence the general validity of this study. The missing values were, therefore, deleted, resulting in a final dataset with no missing data, as shown in Figure 11 within Appendix C.

Data Standardization

For this study, data standardization involved transforming the data to a standard scale without distorting differences in the range of values. This is especially true when we combine the variables of motor impulsivity, openness to experience, and personal information privacy, because they are measured using different measurement units and ranges. In this context, the researcher employs z-score data standardization in Excel to ensure that the dataset collected in this study is suitable for meaningful analysis, especially when variables come from different scales or units.

Validity and Reliability

Determining validity in a study is crucial for maintaining the credibility of the outcomes and ensuring that the variables being measured align with the research questions and objectives of the study (Alrashdi, 2023). Participants in this study anonymously completed the survey on the Qualtrics platform. The participants could withdraw from the study without penalty. The 13-item response scale for the original ABIS impulsivity scale (Coutlee et al., 2014) options were

changed to measure the motor impulsivity dimension on a five-point scale (1 = Never, 2 = Rarely, 3 = Occasionally, 4 = Very Frequently, and 5 = Always). The original five-point Likert scale (e.g., Strongly Disagree to Strongly Agree) does not reflect attitudes or opinions. In contrast to the original scale options, the modified response scale options available in the Qualtrics platform (e.g., "Never" to "Always") measured the frequency of behaviors or experiences. Altering the survey options from a traditional agreement scale to a frequency scale was justified based on the specific goals of this study. Because the purpose of the study was to seek to establish the frequency of the behavior, not to ask respondents about a degree of agreement or disagreement with a statement, the Likert-scale "Always," "Very Frequently," "Occasionally," "Rarely," and "Never" were recast to fit the core research. This change enabled the researcher to see how frequently participants perform or experience various behaviors, thereby providing richer, more actionable information regarding habits. For example, when it comes to the best cloud security practices, it can help to know how often people are doing something safely to gain a better understanding of the authentic security culture and practices within a company. This adjustment made the survey instrument more closely reflect the research questions posed, allowing for more appropriate results that can be applied to practices.

Openness to experience was assessed as the moderator on a 5-point response scale using the BFI-10 (Rammstedt & John, 2007). However, the Qualtrics survey platform with response options: Strongly disagree, Disagree a little, Neither agree nor disagree, Agree a little, and Strongly agree served more relevance to the study. The investigator revised the BFI-10 (Big Five Inventory-10) survey response options "(1 = Strongly disagree, "2 = Disagree a little," "3 = Neither agree nor disagree," "4 - Agree a little," and "5 = Strongly agree) to obtain a more fine-grained response. The original BFI-10 included a Likert scale that might not always accurately

measure minor deviations among respondents' answers to their attitudes (Rammstedt & John, 2007). It expanded the data collection by including the 'Disagree a little' and 'Agree a little' responses, representing a small degree of disagreement or agreement. This variation probably had the effect of minimizing response bias and improving the reliability of the data. Those options allowed respondents to offer opinions in more nuanced shades than the two simplest options: "Strongly disagree" and "Strongly agree." This enhancement mitigated the impact of the central tendency bias, where respondents were more likely to select the mid-point option to avoid the two ends. It also reduced response bias, which occurs when participants tend to agree with statements that they only partially agree with. These new response options ranged from signs of how much one concurred or did not to yield a more moderate estimate for the respondents. The ultimate consequence was a higher-quality and more suitable dataset, resulting in a better research outcome.

Targeted variable HAIS-Q survey scale (Parsons et al., 2014) options were revised for individual behavior assessment with a 5-point response scale (i.e., Strongly Disagree, Disagree, Neutral, Agree, and Strongly Agree). For ease of use, the HAIS-Q scale response options were adjusted to represent the following: "1 = Never," "2 = Occasionally," "3 = Rarely," "4 = Almost always," and "5 = Always." The modification was reasonable as the research scope was related to cloud security practices by technology professionals and business management. This move has contributed to a better understanding of how often employees change their behavior and make secure choices. The original agreement-based scale response options were not suitable for this research, as a frequency-based scale reflected respondents' actual behavior and habits, which was more desirable when studying the patterns and gaps in security behaviors. For example, knowing that many users "occasionally" perform security-related activities while utilizing cloud services

would help provide a focus area for targeted training and policy clarification. The Concern for Information Privacy (CFIP) survey scale (Smith et al., 1996) was used to measure the mediating variable, personal information privacy, using a 5-point scale survey response. The CFIP survey scale options were adjusted to "1 = Strongly disagree," "2 = Disagree a little," "3 = Neither agree nor disagree," "4 = Agree a little," and "5 = Strongly agree" from the response scale of Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree to capture more nuanced responses in the context of cloud business and data security management. By collecting "Disagree a little" and "Agree a little" responses, the researcher can more effectively distinguish the varying degrees of agreement, which is critical in cloud environments, as individuals' concerns about cloud business and data security management can be nuanced and varied, particularly regarding data storage and access control.

The internal consistency of the survey findings across all questionnaire items was analyzed using SPSS reliability analysis to determine Cronbach's alpha. Question 1 represented informed consent and Questions 2-5 denoted demographic profiling. The four instruments that were employed in this study measured four constructs namely openness to experience (Q6_1--Q6_10), personal information privacy (Q7_1--Q7_20), motor impulsivity (Q16_1--Q16_13), and individual behavior (Q17_1--Q17_20). Using SAS software, the reliability analysis was completed amongst the items of each sub-scale to verify their internal consistency. Based on the analysis of internal consistency of the scales, Cronbach's alphas in Table 3 below included ABIS ($\alpha = .72$), CFIP ($\alpha = .73$), BFI-10 ($\alpha = .78$), and HAIS-Q ($\alpha = .76$). Furthermore, Cronbach's alpha showed the questionnaire to reach a higher than acceptable value of 0.7. From the output of SAS reliability analysis for all 63 items, Cronbach’s alpha of .88 obtained overall as shown in Table 3 below (see Figure 12 in Appendix C for more details about SAS output). The researcher concluded that the

research instruments were reliable as the overall Cronbach's alpha of .88 was acceptable and indicated good internal consistency.

Table 3

Reliability Analysis

Scale	Factors (Items)	Cronbach's Alpha
ABIS	MI (13)	.72
CFIP	PIP (20)	.73
BFI-10	OEP (10)	.78
HAIS-Q	IB (20)	.76
Overall	63	.88

Note. MI = Motor Impulsivity; OEP = Openness to Experience; PIP = Personal Information Privacy; IB = Individual Behavior.

In a quantitative study, validity refers to the extent to which the research instruments accurately measure what they are intended to measure. There are several types of validity that researchers consider, such as content, criterion-relation, and construct validity. All of these forms of validity are important in establishing the reliability and applicability of the results, and they were built on the overall credibility of the study. Content validity revealed whether the instrument comprehensively covered all aspects of the construct being studied, which was often evaluated through expert judgment. Since this study was not focused on evaluating the comprehensiveness of the instrument(s) but rather their performance or relationships among constructs, content validity was not a priority and relevant. Criterion-related validity involved determining how well the instrument correlated with an established standard, and it was divided into concurrent validity (comparison with current measures) and predictive validity (ability to predict future outcomes).

This study was not focused on comparing the instrument to a known standard or external benchmark but instead assessed internal constructs or latent relationships; criterion-related validity does apply. However, construct validity assessed whether the instrument truly measured the theoretical construct, incorporating subtypes like convergent and discriminant validity. Convergent validity evaluated whether a measurement correlated strongly with other measures designed to assess the same or similar constructs.

Discriminant validity, on the other hand, assessed whether the measurement has low or no correlation with instruments measuring unrelated constructs. Unlike convergent analysis, discriminant analysis was used to predict categorical outcomes. Since the outcome variable (individual behavior) in this study was continuous and not categorical, thus, discriminant validity was evaluated to perform validity analysis. The construct validity was relevant to this study in ensuring the validity of the questions on the questionnaire, and the construct validity was tested using SAS principal component analysis (PCA), the results of which are shown in Table 4 below. See Appendix C A3 for SAS output details. From the PCA results, it was interpreted that the questionnaire items were clustered into components. The first twelve components were found to have eigenvalues >1, which were meaningful to meet the MINEIGEN criterion and were retained. The proportion column in Table 4 below showed that the first principal component accounted for the most variance of 28.5% with the highest eigenvalue in the data set, and the following two components explained the remaining variance of 15.1% and 10% respectively, in the data set. Overall, a total of over 52% variance was explained by the first three components, and each consecutive component accounted for less and less variance consecutively. The cumulative variance after the first five components was > 69.8%, which demonstrated strong latency structure and substantial tolerance to the construct validity. Additionally, the eigenvalues >1 denoted

profound components, and the validity implied that they matched the theoretical construct count, and the first four components explained the majority of the variance. The diminishing eigenvalue <1 from component 13 onwards implied that those components had insignificant explanation power. See Appendix C A4 for SAS output.

Table 4

Principal Component Analysis

Eigenvalues of the Correlation Matrix

	Eigenvalue	Difference	Proportion	Cumulative
1	17.9723468	8.4551012	0.2853	0.2853
2	9.5272457	3.2242398	0.1512	0.4365
3	6.3030058	0.6084241	0.1000	0.5365
4	5.6945817	1.1887525	0.0904	0.6269
5	4.5058292	0.7182610	0.0715	0.6985
6	3.7875682	1.1721900	0.601	0.7586
7	2.6153783	0.7191862	0.0415	0.8001
8	1.8961921	0.294473	0.0301	0.8302
9	1.6017548	0.1175754	0.0254	0.8556
10	1.4840794	0.372583	0.0236	0.8792
11	1.1114964	0.0997026	0.0176	0.8968
12	1.0117938	0.044312	0.0161	0.9129

Note. First three components accounted for over 53% of the total variance.

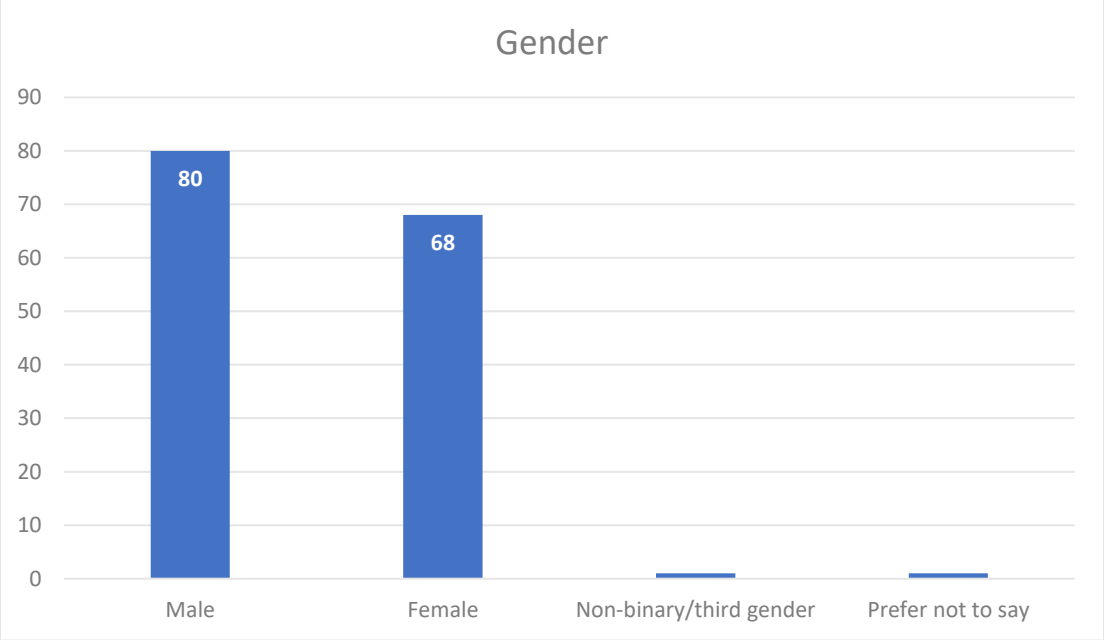
Descriptive Statistics

Sample Demographics

Men and women were included in the study (80 males and 68 females). More men than women chose to complete the survey. Figure 5 illustrated a bar graph of frequency distribution for the gender of the respondents. The gender frequency distribution showed that out of all the respondents, 80 were male, hence the most frequent gender in the study. Female participants followed closely, with 68 females involved in the study. On the other hand, a single participant described themselves as non-binary; this is a gender identity that was not known as male or female. Likewise, 1 respondent decided to choose the no response option for gender.

Figure 5

Bar Graph for the Gender Frequency Distribution



Note. Male participation was higher than female participation.

The study focused on experienced individuals who have worked in technology and networking-related corporates and understand the impacts of networking on human behavior.

The inclusion criterion targeted individuals who have worked for more than 5 years in the company. Based on the demographic information collected, Table 8 below illustrated that 43% of the respondents worked in their current corporation for 6-15 years, 40% have worked for 16-25 years, and 17% have worked for more than 26 years. The researcher included Qualtrics default survey questions to assess IT sector type, which was not part of the initial questionnaire design for this study. Although all the participants were found to be in the IT sector, they are self-reported where they came from different subsectors ranging from technical communication (20%), networking (35%) and cloud computing (45%) and the data as tabulated in Table 5 below. These findings revealed a balanced representation of organizational sectors within the cloud security research field based on the sample of this study. The 45% participation from the cloud computing sector underscored the centrality of this field in cloud security research.

Table 5

Frequencies and Percentages for Organizational Experience

Demographic	Category	%	*n*
Sector	Technical Communications	20	30
	Networking	35	53
	Cloud Computing	45	67
	Total	100	150
Work experience	6-15 years	43	65
	16-25 years	40	60
	26 and above	17	25
	Total	100	150

Note. Participants range from 6-26 years of cloud security experience.

As cloud computing and cloud security are inextricably connected, it made sense that cloud security employees were the most involved. These findings critically contributed to facilitating and optimizing cloud data and services security mechanisms and the high percentage

strongly emphasized the practical aspects of cloud security measures and their effect on cloud infrastructure. Networking professionals also had a unique comprehension of the infrastructure underpinning cloud services, which were critical for securing data as it traversed networks. Their involvement helped to ensure that security policies were broad and included the cloud and networking security attack vulnerabilities. Similarly, 20% were the technical communications professionals that do their part in disseminating security practices and protocols across the organization. As a whole, these broad pillars make for a holistic approach to cloud security, one that was based on practical application, infrastructure management, and open dialogue.

The investigator also gathered information on cloud security technology professionals, managers, and executives employed within cloud security networking organizations in the United States. Regarding participant roles, about 13% were executives, business and IT, 26% were managers, business and IT, and 61% were cloud security professionals - including analysts, engineers, and architects. These results underscore the varied work in the realm of cloud security. Given that 61% of survey respondents were cloud security practitioners who operated cloud security controls, most were actively involved in cloud security's technical and implementation details.

This high ratio represented a great deal of practical, real-world experience – and expertise – crucial in solving challenging, real-world problems in cloud security. The population of 26% also shows that many managers were making strategic decisions to drive the discipline of cloud security. Managers were an integral link between technical system administrators and decision-making executives, as they were tasked with mapping security processes to the organization's strategic goals and the regulators' mandates.

Table 6

Frequencies and Percentages for Cloud Business and Security Job Roles

Type of Role	%	*n*
Business Executive	1	2
IT Executive	12	18
Business Manager	22	32
IT Manager	4	6
Cloud Security Analyst	45	67
Cloud Security Architect	3	5
Cloud Security Engineer	13	20
Total	100	150

Note. Executives: 13%; Managers: 26%; Professionals: 61%.

In Table 6 above, 13% of participants who call themselves executives in business and IT reflected their involvement at high levels of decision-making in cloud security activities. It was imperative for organizational commitment that strict security measures be maintained, and essential resources secured. With executives engaged in cloud security, one notes a senior-level recognition of its importance in an enterprise. That could lead to additional comprehensive and better-funded security plans for everyone else on the line. These results reveal that all kinds of professionals participated in this study, and each brought new and different kinds of knowledge, perspective and experience to help secure cloud business and security infrastructure. Together, participants' job roles provided a comprehensive view of how impulsivity, personality traits, and privacy concerns influenced cloud security behavior across operational and strategic levels.

Measures of Central Tendency: Mean, Median, Mode

Measured in terms of data analysis, indices including mean, median, and mode was important for describing the features of a data set. These measurements were one effective ways to gain insight into what values were typical and the general trend of the dataset. They provided a basis for knowing what auxiliary statistical procedures were appropriate. The mean (or average) was found by adding all the values together, then dividing by the number. It was a fast estimate of the center of the data. However, it can be sensitive to outliers, which can skew the mean and make it less representative of the majority of the data points.

Table 7

Descriptive Summary Statistics for the Standardized Variables in the Study (N = 150)

Variable	Min	Max	*M*	*Mdn*	Mode	*SD*
Motor impulsivity (MI) - predictor	1	4	2.01	2.00	2	0.69
Openness to experience (OEP) – moderator	3	5	3.40	4.00	3	0.48
Personal information privacy (PIP) – mediator	2	5	3.86	4.00	4	0.52
Individual behavior (outcome)	2	4	2.87	2.98	3	0.51
MI*OEP	3	17	6.94	6.30	6	2.99
MI*PIP	3	17	7.73	7.35	4	2.83

Note. The interaction variables are MI*OEP and MI*PIP.

Table 7 above showed the mean, median, and mode for the predictors, criterion, and interaction variables, which were standardized using z-scaling procedure. Analyzing the summary statistics for the independent variable, motor impulsivity, where the response set range was 1 = Never, 2 = Rarely, 3 = Occasionally, 4 = Very Frequently, and 5 = Always, the mean

value of 2.01 suggested that, on average, individuals reported "Rarely" engaging in impulsive behaviors related to cloud security management. The fact that the median was equal to 2, equal to the mean also validated that central tendency of response was "Rarely". Furthermore, the mode of 2 meant "Rarely" and it was the most common response of the participants. This uniformity between the mean, median, and mode points out to an overall tendency of decreased impulsivity among participants; a feature that was favorable to cloud business and security behavior as this suggested more conscious and non-imperative decision-making. It was this type of behavior that was key in maintaining strong security rules and lessens the risk of snap decisions that could jeopardize security. measures. This observation was an important knowledge of the behavior among the study sample, which showed that as a rule organizations were still more cautious towards the management of cloud security.

For the moderator variable, openness to experience where the survey response options were 1 = Strongly disagree, 2 = Disagree a little, 3 = Neither agree nor disagree, 4 = Agree a little, and 5 = Strongly agree, and given the mean value of 3.40 suggested that, on average, respondents were close to “neither agree nor disagree” when it came to openness to experience. The median value of 4 indicated that at least half of the participants actually leaned towards "Agree a little," showing a tendency towards being open to new experiences. Mode of 3, indicated "Neither agree nor disagree" , which emphasized that this answer was the most common among the sample. This distribution implied that a substantial number of the sample were indifferent to novel ideas and experiences.

However, the mediator variable, personal information privacy, where the response options ranged from 1 = Strongly disagree, 2 = Disagree a little, 3 = Neither agree nor disagree, 4 = Agree a little, and 5 = Strongly agree, the mean value was 3.86, which suggested that, on

average, respondents leaned towards "Agree a little" when it came to concerns about personal information privacy. The median value of 4 confirmed that at least half of the samples held this view, showing employee concern about personal information privacy. The mode of 4 indicated the most common response, continued to accept personal information privacy. This asymmetry indicated a strong bias against self as recipient of personal privacy information. Understanding these attitudes was essential for cloud security management because it indicated the role an individual professional played in the secure protection of their data. The focus on privacy therefore only can result in demands for tighter controls and rules inside clouds to protect data.

In a similar broad picture, the survey responses whose rating items were: 1 =Never, 2= Rarely,3 =Occasionally, 4 = Almost Always, 5=Always for the dependent variable, such as individual behavior, the mean 2.87 determined that at this point, sharing somewhat most of the respondents were "rarely" engaged in security practices. The median value of 2.98 alluded to an aggregated regularity for individual behavior, "Rarely." While the most frequently occurring mode scores were closer to the mean, in other words, since the mode's overall tendency still leans on the side of 3, it can be inferred that "Rarely" was the predominant behavior for these participants.

In all three indices, there was a gentle decline from gentle to moderate: "Rarely" becoming slightly less so through "Occasionally" (with 0.5 =more often) then the point near zero lying below 'occasionally but above 'rarely.' At this juncture, trends in such cloud security behavior statistics indicated that something more optimistic than a moderate level of engagement may evolve. Something more at stake than a moderate level of engagement with cloud security can be read into this trend. Furthermore, an individual who occasionally paid attention or took advantage of security practices seemed desirable from the point of view of cloud security

management. Since there were indications that some professionals engaged very infrequently or even never with security practices, this outcome made one pause to consider whether to shift business priorities toward promoting less disturbance in bringing consistent and pro-claim behavior with even better security assurances. Moreover, overall estimates were available in the lines that described the standardized interaction variables for motor impulsivity and openness to experience in Table 7 above. The mean of 6.94 for the interacted variable MI*OEP equaled approximately one standard deviation. The median value, near the mean at 6.30, suggested a central tendency for these data. Although the mean or most likely value does not capture average levels of interaction, it provides a rough picture. A mode of 6 was the most frequently occurring value in the distribution. Once again, this emphasized the main finding above. With such a distribution, while there may be variety concerning how motor impulsivity interacted with openness in an individual's behavior, most individuals fell between the two.

However, professionals with such balanced levels of openness to experience and motor impulsivity could be standard throughout the sample, and this meant that the security behaviors they follow will likely be diverse but adaptable as well. Understanding this interaction will help determine common behavior patterns and aid in managing such patterns to improve cloud security and data management. Also, this study examined the summary statistics for standardized interaction variables of motor impulsivity and personal information privacy (MI*PIP) in the context of cloud security. With a mean value of 7.73, it can be concluded that these traits in combination result in behavior which is, on the whole, closer to "Occasionally". The approximate mean of 7.35 suggested this nature of the average result was close to something in between "Occasionally" and "Rarely." The mode of 3, which was the value that most frequently occurred, reconfirmed the concept of the most common response being that "Rarely" among

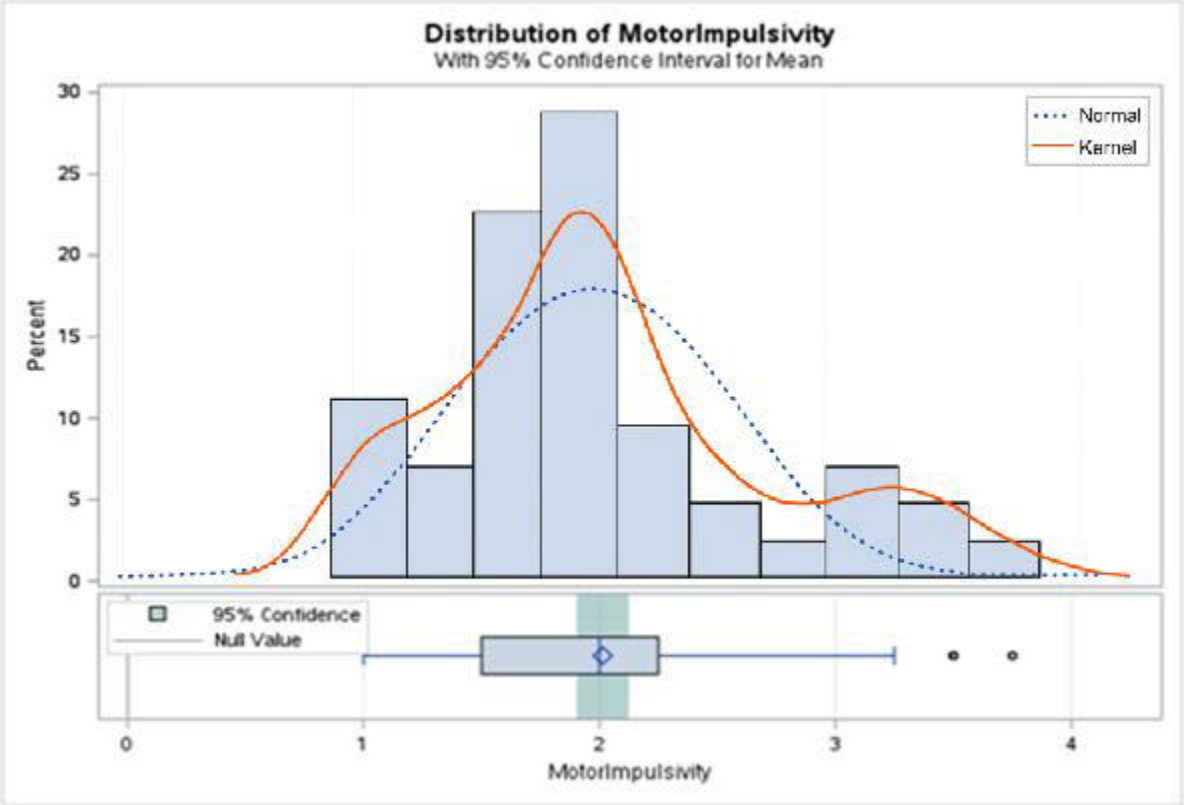
respondents. Personal information privacy had a medium trend and frequency in conjunction with occasional impulsiveness. Grasping these interactions was a crucial step in shaping cloud security and data management strategies that cover impulsive individual behavior and personal information privacy concerns, allowed a balanced look at security risks to prevail.

Outliers Detection and Treatment

To ensure validity and reliability of statistical analyses, outliers detection and treatment was a critical step. Henceforth, boxplots were created in SAS to visually inspect extreme values.

Figure 6

Independent Variable: Motor Impulsivity

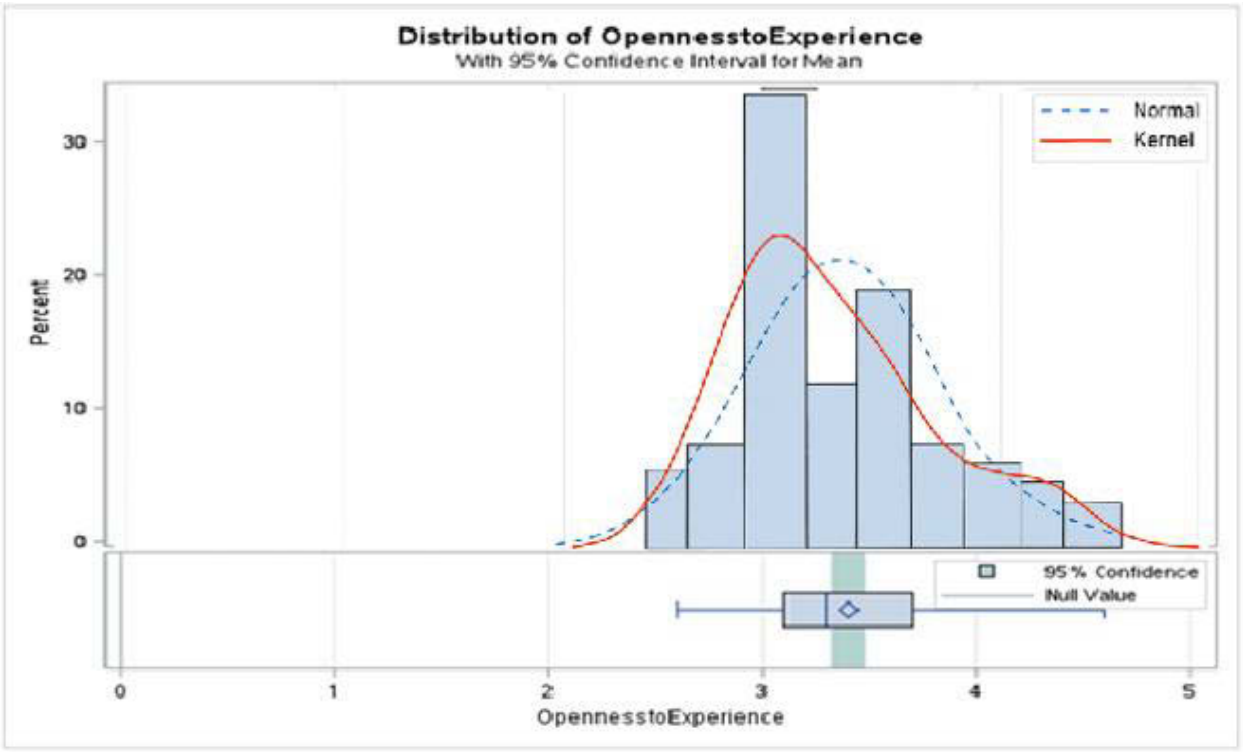


Note. Right skewed two outliers indicated rare extreme values.

If extreme values were found the dataset then z-score analysis was conducted to determine if the value to be retained or removed to further preserve data integrity. In this study, the z-scores falling within the range of -1 to +1 were considered not to be outliers. Figure 6 above included two extreme values next to the right whisker in a box plot for motor impulsivity, which suggested that the vast majority of the data was concentrated towards lower values, with only a few cases displaying high impulsivity scores. The range of *z* scores for these two cases were examined, and they were found to be less than 1. Thus, the two cases were determined to not be outliers. However, Figure 7 below showed the graphs for the moderator variable, openness to experience. There were no outliers towards any whiskers in the box plot for openness to experience. This indicated a consistent distribution without extreme deviations in responses.

Figure 7

Moderator Variable: Openness to Experience

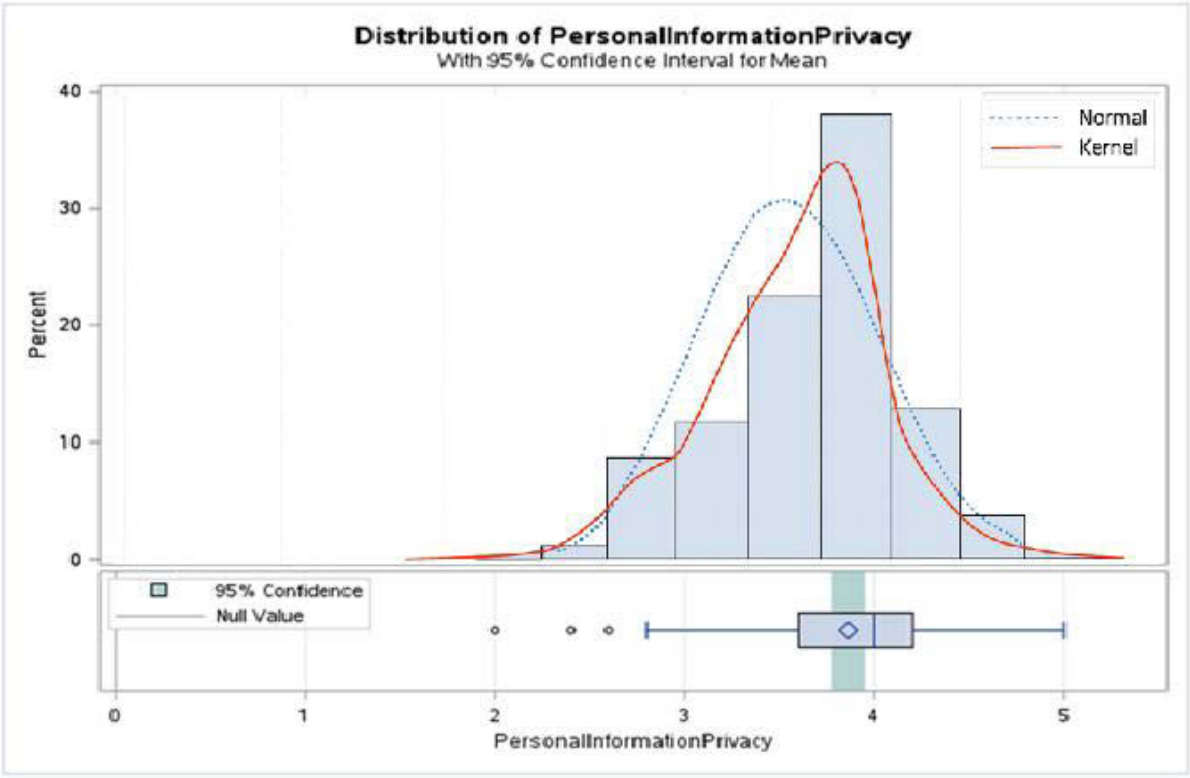


Note. No extreme values found indicating homogenous distribution.

Figure 8 below for personal information privacy showed three possible extreme values towards the left whisker in a box plot. An examination of the range of *z* scores for these three cases was found to be less than 1. The z-scores falling within the range of -1 to +1 were considered not to be outliers. Thus, the three cases showed as extreme values were determined to be not outliers and as such, they were included in the subsequent analysis.

Figure 8

Mediator Variable: Personal Information Privacy



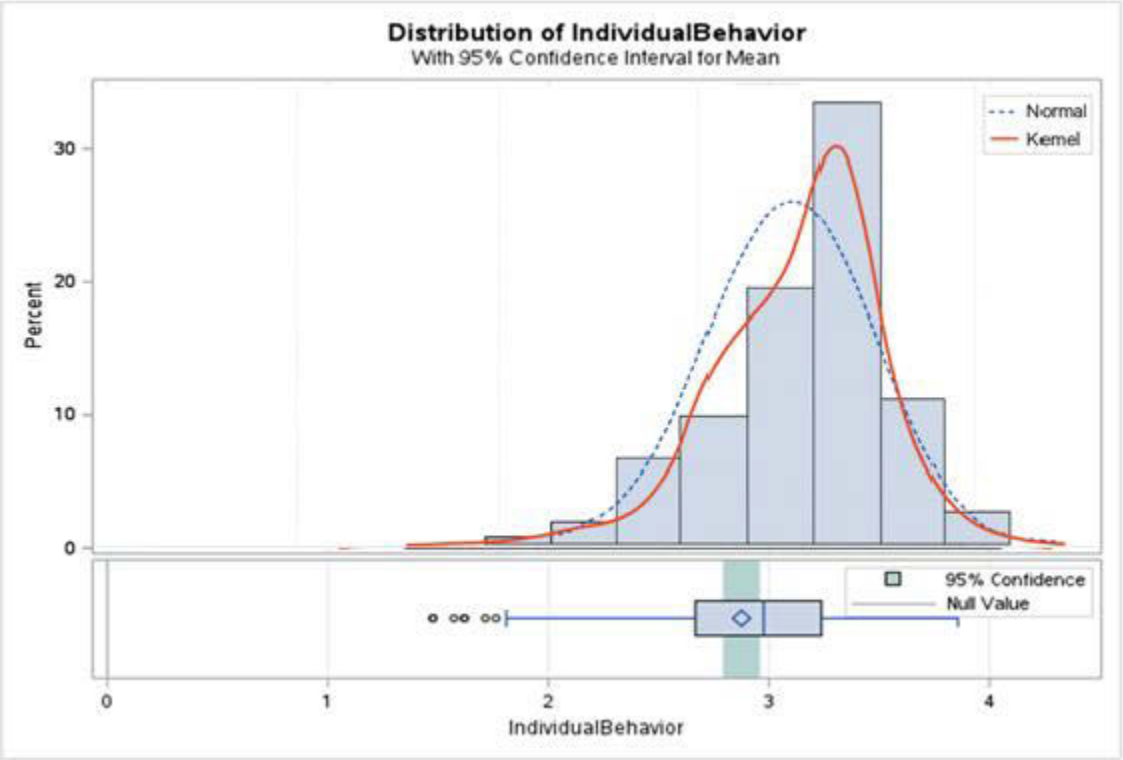
Note. Left skewed outliers indicated contrast to the majority.

Similarly, Figure 9 below showed five extreme values towards the left whisker in a box plot for the outcome variable, individual behavior. An examination of the range of *z* scores for these five cases indicated less than 1, which was within the cut off range of 1 to +1. Thus, the researcher

determined that these cases were not outliers and as such, they were included in the subsequent analysis. On the other hand, after looking at z scores of potential outlying values, the researcher defended keeping the outlying values in their place and preserving the fidelity of the model to the source data and not to the researchers' "convictions".

Figure 9

Outcome Variable: Individual Behavior



Note. Left skewed values clustered around less than 1 indicated no outliers.

Statistical Assumptions Testing

Normality Test

To test whether the normality was statistically significant given the data was tested with null hypothesis normality with α =. 05. One-sample two-tailed t-test for normality testing was applied in SAS, then p value was calculated as below

Hypothesis Testing.

H_0: data was normally distributed.

H_a: data was not normally distributed.

Table 8

Shapiro-Wilk Values for Study Variables

Variable	Shapiro-Wilk Value	*p*
Motor impulsivity (MI) - predictor	0.924	< . 001
Openness to experience (OEP) - moderator	0.946	< . 001
Personal information privacy (PIP) - mediator	0.958	< . 001
Individual behavior (outcome)	0.934	< . 001

Note. All study variables violated statistical normality assumption as Shapiro-Wilk p <.001.

Based on the results in Table 8 above, the Shapiro-Wilk test p value is < .0001. Since the p value < .05 for all the study variables (motor impulsivity, openness to experience, personal information privacy, and individual behavior), the null hypothesis was rejected and concluded that the data were not normally distributed. Thus, there was sufficient evidence and 95% confident that the normality condition was violated, and the random samples were not from normal distribution population. The Shapiro-Wilk test assessed whether the distribution of a variable deviated from a normal distribution. In this case, the extremely low p value suggested that the data was not normally distributed. By acknowledging and treating the violation of the normality assumption, the researcher employed alternate approaches such as Box-Cox transformation (see Figure 15 through Figure 18 within Appendix C). Table 9 below showed Box-Cox transformed Shapiro-Wilk p-values >.05, which suggested that the random samples were from the normal distribution population and normally distributed.

Table 9

Shapiro Wilk Values for Study Variables After Box-Cox Transformation

Variable	Shapiro-Wilk Value	*P*
Motor impulsivity (MI) - predictor	0.9967	0.5778
Openness to experience (OEP) - moderator	0.9948	0.1752
Personal information privacy (PIP) - mediator	0.9942	0.1165
Individual behavior (outcome)	0.9965	0.5209

*Note. S*tatistical normality assumption was met as Shapiro-Wilk $p > .001$.

Collinearity Test

In multiple linear regression, where the predictor variables such as motor impulsivity (MI), interacted variables (MI*OEP & MI*PIP) were involved in this study, there could be phenomenon that these predictors can highly correlate with each other obscuring their attribution to the variance.

Table 10

Multicollinearity Test

						Collinearity Statistics	
Variables	*B*	*SE*	*β*	*t*	*p*	Tolerance	VIF
Intercept	3.334	0.131	0	25.500	<.001	0	0
MI	-0.114	0.141	-0.152	-0.809	0.420	0.17	5.75
MI*OEP	-0.009	0.015	-0.052	-0.636	0.526	0.92	1.09
MI*PIP	-0.030	0.034	-0.164	-0.872	0.385	0.17	5.77

Note. VIF values of MI, MI*OEP, MI*PIP VIF values are less than 10 and Tolerance is greater than 0.1.

The researcher assessed the multicollinearity of variables using the VIF method by running the linear regression analysis in SPSS to test if the VIF value was greater than 10 and Tolerance was less than 0.1 then it would be concerning that multicollinearity existed in the study data set. See Figure 19 for more details about the SPSS output in Appendix C. Table 10 above showed Tolerance and VIF values for the predictors including MI, MI*OEP, and MI*PIP. Based on the results in the Table 10 above, the researcher concluded that the data met the assumption of collinearity indicating that multicollinearity was not a concern (MI, Tolerance = .17, VIF = 5.75; MI*OEP, Tolerance = .92, VIF = 1.09; MI*PIP, Tolerance = .17, VIF = 5.77). The researcher also checked to see if the residual terms were uncorrelated by locating the Model Summary table and the Durbin-Watson value in SPSS linear regression analysis if the value was as close as 2. See Figure 19 in Appendix C for the SPSS output of the Model Summary. Table 11 below displayed Durbin-Watson value, which was closer to 2, thus, the data met the assumption of independent errors (Durbin-Watson value = 2.167).

Table 11

Model Summary – Independent Errors

Outcome Variable	*R*	R^2	*Adjusted* R^2	*SE*	*Durbin-Watson*
1	0.327	0.107	0.088	.495	2.167

Note. Predictors: (Constant), MIPIP, MIOEP, MI; Dependent Variable: IB.

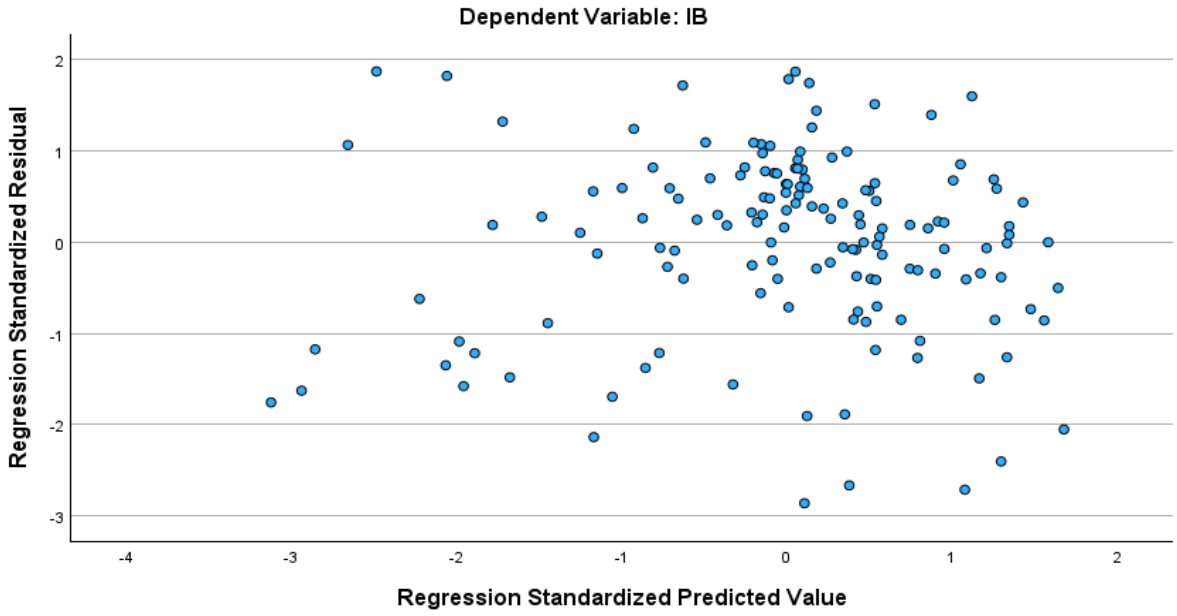
Homoscedasticity Test

To test homoscedasticity assumption that the variance of the residuals (the differences between observed and predicted values) was constant across all levels of the independent variables including MI, MI*OEP, and MI*PIP in the regression model, the researcher used two

methods: graphical and analytical to check homoscedasticity for the study data set. A linear regression analysis was conducted in SPSS and the Figure 10 below showed graphical representation of scatter plot of standardized residuals revealing the points were almost evenly spread around the horizontal axis forming a rectangular shape. Additionally, the scatterplot of standardized predicted values showed that the data met the assumptions of homoscedasticity. However, analytical testing was conducted to test statistical significance. See Figure 20 in Appendix C for SPSS ANOVA output of Breusch-Pagan test.

Figure 10

Scatter Plot of Standardized Residuals



Note. Predictors: (Constant), MIPIP, MIOEP, MI; Dependent Variable: IB.

The Breusch-Pagan test was a statistical method used to detect heteroscedasticity in a regression model, which occurs when the variance of residuals is not constant across levels of the independent variables. The researcher performed Breusch-Pagan test in SPSS by first opening the study dataset, selecting predictor variable (MI) and the independent variables including

interacted terms (MI*OEP & MI*PIP), and checking unstandardized predicted values and residuals boxes in the linear regression. A multiple linear regression model was fit and both the predicted values (PRE_1) for each observation and the residuals (RES_1) were shown in two new columns in the Data View window. See Figure 20 within Appendix C for SPSS data view showing predictor and residual values. Next, the squared residuals were computed using Transform and Compute options in SPSS. See Figure 21 in Appendix C for SPSS squared residuals computation. Then the researcher ran the regression analysis to determine if there were unequal variances (heteroscedasticity) in this study dataset.

Table 12

ANOVA Breusch-Pagan Test

Model 1	*Sum of Squares*	*df*	*Mean Square*	*F*	*P*
Regression	0.620	3	0.207	1.667	0.177
Residual	18.111	146	0.124		
Total	18.731	149			

Note. ANOVA p-value is >0.05.

Hypothesis test procedure was outlined below to determine the p-value:

H_0: $\sigma_1 = \sigma_2 = \sigma_3$

H_a: $\sigma_1 <> \sigma_2 <> \sigma_3$

where σ_1 = MI, σ_2 = MI*OEP and σ_3 = MI*PIP

See Figure 22 in Appendix C for SPSS ANOVA output. To prove the assumption of homoscedasticity that there was no difference in the levels of variability between the predictor variable (MI) and the interacted terms (MI*OEP & MI*PIP), the researcher ran the following

hypothesis to test those variances with $\alpha = 0.05$. Based on the Breusch-Pagan test results as illustrated in Table 12 above, the p-value was 0.177. Since the p-value was more than 0.05, the researcher had no reason to conclude heteroscedasticity existed in the regression model and the null hypothesis was rejected. Therefore, there was statistical evidence and 95% confidence that homoscedasticity assumption was fulfilled.

Mediation Analysis

The main objective of the mediation model was to test any potential dealing that personal information privacy concern played between the two research constructs and their relationship between motor impulsivity and individual behaviors in managing cloud business and security. Through investigating this potential mediating hypothesis, the study attempted to ascertain whether concerns about privacy played a dominant role in how motor impulsivity correlated with behavior towards cloud security. Understanding this mediation effect was particularly important, as it can offer a stronger understanding of how impulsive tendencies affect cloud security behaviors and guide more pragmatic strategies to manage these behaviors:

RQ1: Does motor impulsivity impact individual behavior in cloud business and data security management?

$H1_0$: Motor impulsivity does not significantly impact individual behavior in cloud security management.

$H1_a$: Motor impulsivity significantly impacts individual behavior in cloud security management.

$H2_0$: Personal information privacy does not significantly mediate the relationship between motor impulsivity and individual behavior in cloud security management.

$H2_a$: Personal information privacy significantly mediates the relationship between motor impulsivity and individual behavior in cloud security management.

The mediation analysis was conducted using SPSS's PROCESS macro (Hayes & Scharkow, 2013). See Figure 23 and Figure 24 in Appendix C for further details on SPSS outputs. Table 13 below showed the model summary of the independent variable (MI) predicting the target variable (IB) and the mediator variable (PIP). The overall model predicting IB was statistically significant, $F(2, 147) = 6.16$, $p = .0027$ and it accounted for 7.73% of the variance in IB ($R^2 = .0773$). Similarly, the model for MI predicting PIP was statistically significant, $F(1, 148) = 8.11$, $p = .0050$, and it accounted for 5.19% of the variance in PIP ($R^2 = .0519$).

Furthermore, Table 13 below showed the mediation analysis results where MI (B = -0.31, p = .047) revealed a significant negative relationship between MI and IB ($t = -2.10$, $t = 10.81$). For every unit increase in MI, IB decreases by 0.31 on average. Since the direct effect of the independent variable, motor impulsivity (MI) is statistically significant and impacted the outcome variable, individual behavior (IB), the researcher failed to accept the null hypothesis. In other words, motor impulsivity impacted individual behavior in cloud security management. Thus, the null hypothesis $H1_0$ was rejected.

Table 13

Regression Model Summary for MI Predicting PIP (N = 150)

Outcome Variable	*R*	R^2	*MSE*	*F*	*df1*	*df2*	*P*
IB	0.2781	0.0773	1.4435	6.1601	2.0000	147.0000	0.0027
PIP	0.2279	0.0519	0.3641	8.1073	1.0000	148.0000	0.0050

Note. Both models are significant (p<.05).

Table 14

Mediation Analysis

Path	*B*	*SE*	*β*	*t*	*p*	95% Confidence Interval for *B*	
						Lower Bound	Upper Bound
Intercept	5.82	0.54	0	10.81	0.000	4.762	6.893
MI ⟶ IB (Direct)	-0.31	0.15	-0.31	-2.10	0.048	-0.609	-0.004
MI ⟶ PIP	-0.21	0.07	-0.21	-2.85	0.005	-0.36	-0.07
PIP ⟶ IB	-0.53	0.16	-0.53	-3.26	0.001	-0.86	-0.21
MI ⟶ IB (controlling PIP)	-0.31	0.15	-0.31	-2.01	.048	-0.61	-0.00

Note. MI = motor impulsivity; PIP = personal information privacy; IB = individual behavior.

Table 14 above also showed the direct effect of PIP (B = -0.53, p = .001) on IB indicating a significant negative relationship between PIP and IB (t = -3.26, t = 10.81).

Table 15

Bootstrap Mediation Effects of PIP on IB with 95% Cis for 5000 Bootstrapped Samples

Path	*B*	*BootSE*	95% Confidence Interval for *B*	
			BootLLCI	*BootULCI*
Indirect effect (unstandardized)	0.11	0.05	0.03	0.24
MI ⟶ IB	0.31	0.05	4.76	6.89

Note. Indirect effect = MI ⟶ IB (controlling PIP).

Since the regression coefficient between motor impulsivity (MI) and individual behavior (IB) was statistically significant, as was the regression coefficient between personal information privacy (PIP) and IB, the researcher tested the significance of this indirect effect using

bootstrapping procedures in SPSS. Table 15 above indicated unstandardized indirect effects of PIP that were computed for each of 5,000 bootstrapped samples at 95% confidence intervals. Since the bootstrapped unstandardized indirect effect of PIP was .11, and the 95% confidence interval ranged from .03 to .24, the indirect effect was statistically significant. Overall, the mediation analysis from Table 18 above established that motor impulsivity (MI) had a significant direct effect on individual behavior (B = 0.31, 95% CI [4.76, 6.89], and a significant indirect effect of PIP (B = 0.11, 95% CI [0.03, 0.24]. This set of findings implied that personal information privacy played a significant mediating role in the association between motor impulsivity and behavior. Thus, the researcher rejected $H2_0$ null hypothesis.

Moderation Analysis

The objective of this moderation analysis was to examine whether openness to experience considerably influenced the strength or direction of the relationship between motor impulsivity and personal behavior in the context of cloud business and security management. Through the investigation of this moderation hypothesis, it was determined whether individuals characterized by different degrees of openness to experience will demonstrate varying behavior in response to their impulsive inclinations. Understanding this moderate effect was important, it can uncover subtle interactions that drive behavior among cloud security business and security may expose how personal trait affected the management and compliance of security practices.

> RQ2: How does privacy of personal information mediate, and how does the Big Five personality trait of openness to experience moderate, the relationship between motor impulsivity and individual behavior in cloud business and data security management?

$H3_0$: Openness to experience does not significantly moderate the relationship between motor impulsivity and individual behavior in cloud business and data security management.

$H3_a$: Openness to experience significantly moderated the relationship between motor impulsivity and individual behavior in cloud business and data security management.

The moderation analysis was conducted using SPSS's PROCESS macro (Hayes, 2013). The moderation analysis examined the influence of motor impulsivity (MI) and openness to experience (OEP) on individual behavior (IB) and whether OEP moderated the relationship between MI and IB. See Figure 25 in Appendix C for further details on SPSS outputs of moderation analysis. Table 16 below revealed the regression model summary, which included centered predictor (MI), centered predictor (OEP), explained 56% of the variance in IB (R^2 = .5564), $F(3, 146) = 6.5195$, $p = .0000$. In the second step of the regression analysis, the interaction term (Int_1) between MI and OEP explained 1.8% of the variance in IB (R^2 = .0184), $F(1, 146) = 6.0427$ $p = .0151$.

Table 16

Regression Model Summary Predicting IB (N = 150)

Model	R^2	*F*	*df1*	*df2*	*p*
MI, OEP	0.5564	61.0501	3.0000	146.0000	0.0000
MI, Int_1	0.0184	6.0427	1.0000	146.0000	0.0151

Note. Adjusted ΔR^2 variance = 2% after the interaction with significance ($p<.05$); Int_1 = MI*OEP.

Furthermore, Table 17 below shows all the *p* values of MI, OEP, and Int_1 were statistically significant ($p \leq .05$). MI ($B = 0.2630$, $p = .0000$), which indicates a significant positive

relationship between MI and IB (t = 12.85, t = 28.84), respectively. For every unit increase in MI, IB increased by 0.2630 on average.

Table 17

Moderation Analysis

Variables	*B*	*SE*	*t*	*p*	95% Confidence Interval for *B*	
					Lower Bound	Upper Bound
Intercept	6.0147	0.2085	28.8423	0.0000	5.6025	6.4268
MI	0.2630	0.0205	12.85	0.0000	0.2226	0.3035
OEP	-0.0008	0.0003	-2.9849	0.0033	-0.0014	-0.0003
Int_1	0.0001	0.0000	2.4582	0.0151	0.0000	0.0001

Note. MI = motor impulsivity; OEP = openness to experience; IB = individual behavior;Int_1 = MI*OEP.

On the contrary, OEP (B = -0. 0008, p = . 0033) revealed a significant negative relationship between OEP and IB (t = -2.98, t = 28.84) respectively. For every unit increase in MI, OEP decreased negligibly on average. The interaction between MI and OEP, Int_1 was statistically significant (p =.0000, p = .0000), which meant that OEP moderated the relationship between MI and IB. Additionally, Table 18 below directed the conditional effects of the motor impulsivity relationship at values of the moderator, and openness to experience were significant ($p \leq 0.05$) at levels -887.7267, .0000, and 887.7267 (*SD*, *M*, +SD). Additionally, the results from Regression Model Summary in Table 19 above indicated that the addition of the interaction term Int_1 (R^2 = .0184) explained an additional 2% of ΔR^2 variance, (F(1, 146) = 6.042, p = .0184 in IB, bringing the total to 58%. These findings suggested that the openness to experience moderated the relationship between motor impulsivity and individual behavior. Based on the moderation analysis, the researcher rejected the $H3_0$ null hypothesis.

Table 18

Conditional Effects of MI at Values of OEP

					95% Confidence Interval for *B*	
OEP	*Effect*	*SE*	*t*	*p*	Lower Bound	Upper Bound
-887.7267	0.2177	0.0203	10.7358	0.0000	0.1776	0.2578
0.0000	0.2630	0.0205	12.8492	0.0000	0.2226	0.3035
887.7267	0.3083	0.0332	9.2738	0.0000	0.2426	0.3740

Note. All effects are significant (p<.05).

Hypothesis Test Results

The researcher explored the complex relationships between motor impulsivity, personal information privacy, personality trait such as openness to experience, and individual behavior in cloud security management. Three key hypotheses were tested using SPSS's PROCESS macro (Hayes, 2013)mediation and moderation analysis approach and the results were illustrated in the earlier sections of this thesis.

Table 19

Hypothesis Results

Null Hypothesis	Relationship Tested	Statistical Tests	Results	Status	Reason
$H1_0$	Motor impulsivity does not significantly impact individual behavior in cloud security management.	Mediation Analysis	MI and IB (p = .047, p = .000)	Rejected	p < significance level (.05) revealing motor impulsivity significantly impacted individual behavior

Null Hypothesis	Relationship Tested	Statistical Tests	Results	Status	Reason
$H2_0$	Personal information privacy does not significantly impact the relationship between motor impulsivity and individual behavior in cloud security management.	Mediation Analysis	Mediation effect (0.1140) and Bootstrap Confidence Interval (0.03, 0.23)	Rejected	The positive coefficient indicates that the indirect effect contributed to the increasing impact on individual behavior, and the Bootstrap values reveal the statistical significance of the indirect impact in supporting the presence of mediation.
$H3_0$	Openness to experience does not significantly impact the relationship between motor impulsivity and individual behavior in cloud security management.	Moderation Analysis	Interacted term, Int_1 ($p = .00$, $p = .00$)	Rejected	The interaction between motor impulsivity and openness to experience, Int_1 is statistically significant ($p < .05$) predicting individual behavior supporting the presence of moderation

Note. All of the three null hypotheses were rejected.

The hypothesis results were summarized in Table 19 above along with the reasons for acceptance or rejection of the null hypothesis. For Hypothesis $H1_0$ the researcher rejected the null hypothesis, indicating that motor impulsivity played a crucial role in predicting individual behavior, and predominantly, there was significant impact on the outcome of individual behavior. Similarly, the test results for Hypothesis $H2_0$ steered to reject the null hypothesis. The $H2_0$ test results demonstrated that personal information privacy significantly mediated the relationship between motor impulsivity and individual behavior. The mediating role of positive mediation supported its important significance in the impact of personal information privacy on

individual behavior and an important role in cloud security behavior and encouraged the development of anti-impulsivity measures. As a result, Null Hypothesis $H3_0$ was also rejected because the data reveal that openness to experience significantly altered the motor impulsivity of individual behavior. The significant interaction suggested that the influence of motor impulsivity on individual behavior depended on an individual's level of openness to experience. This subtle result suggested that other personality dispositional characteristics such as openness to experience and motor impulsivity can be influential in potential firms wishing to govern individual activities with regards to cloud security and data administration. In summary, the closing implication was that greater consideration should be given in research to both impulsivity and alternative character differences.

Conclusion

Overall, the researcher argued for the co-existence of motor impulsivity, personal privacy information, and cloud security behavior. By statistical means such as mediation test, their analysis combined with moderation test contributed to exploring the salient factors as well as the interactions among these three factors. The strong influence of motor impulsivity on individual behavior served as a reminder of the need for intervention in impulsive vulnerability factors which yield better security practices in cloud business and security management. To sum up, the groundwork of this chapter was discussed in more detail in Chapter 5, with a number of applications to business organizations, particularly those that concern cybersecurity. By understanding the complexity of these connections and addressing them systematically, providing a safer business environment along to reducing data risks. While at the same time reduced their exposure to risks to their business. In this way, it both shielded sensitive information, and promoted positive behaviors.

Chapter 5: Conclusions, Implications of the Study, and Recommendations

The study examined the impact of impulsivity on employee behavior in cloud business and data security management, focusing on the general assumption that human behavior was an important basic factor that could lead to vulnerabilities in cloud business and data security and business risk. In particular, the study focused on the association between motor impulsivity (predictor) and individual behavior (outcome) in cloud business and data security management and examined the moderating role of openness to experience and the mediating role of personal information privacy. This composite was assessed by Alsharida et al. (2023), to shed some new light on a relationship which has so far not been described in detail.

The statistical results contributed to understanding how the moderation and mediation factors interacted and impacted individual behavior and cloud business and data security management. The chapter was structured into significant parts to examine the research results in-depth and conclude with the results, discussing the findings, future research direction suggestions, and practical and theoretical implications. The discussion ended with a note of study limitations and conclusions, which presented a synthesis of the research input to security behavior. However, the primary research questions that guided this investigation were:

RQ1: Does motor impulsivity impact individual behavior in cloud business and data security management?

RQ2: How does privacy of personal information mediate, and how does the Big Five personality trait of openness to experience moderate, the relationship between motor impulsivity and individual behavior in cloud business and data security management?

Summary of Results

The present study focused on the existing problem of uncertainties regarding the potential effect of motor impulsivity on individual behavior, the moderating role of a Big Five trait, and the indirect effect of personal information privacy. The results gave important suggestions on motor impulsivity, openness experience with, personal privacy discussion and individual behavior in cloud business management and data security control. The statistical test results were significant in the three tested hypotheses, thus clearly indicating the correlation between the study variables. This rejection of the null hypothesis $H1_0$ suggested that motor impulsivity had significant negative influence on individual behavior from a cloud resources' business and security management perspective. This observation indicated that higher levels of motor impulsivity are associated with individual behaviors that can undermine security measures and increase risks to business and data security.

The mediation analysis of null hypothesis $H2_0$ showed that personal information privacy showed a significant partial mediating relationship between motor impulsivity and individual behavior. The partial mediation effect imply that although privacy concerns mediated the relationship between impulsivity and security behavior, the direct impact of motor impulsivity was still rather extensive and significant. The result indicated that the security decision-making processes were multifaceted and have various channels through which impulsivity affected individual behaviors. The partial mediation effect of personal information privacy between motor impulsivity and individual behavior has theoretical contributions to the field because it enhanced the comprehension of behavioral dynamics in cloud business and data security. In other words, privacy concerns played a crucial intermediary role in how motor impulsivity influenced individual behavior, highlighting that the direct impact of impulsivity was predominant. Overall,

the mediation analysis uncovered a significant direct relationship between motor impulsivity and that individuals with higher impulsivity exhibited behaviors that could affect cloud business and data security management and practices. In null hypothesis $H3_0$, the moderation analysis established that openness to experience as one of the personality traits intensely moderated the correlation between motor impulsivity and personal behavior. The critical effect of the interaction demonstrated that the influence of motor impulsivity on individual behavior is diverse and depends on the degree of openness to experience in a specific individual. The moderation results indicated that personality traits were essential in influencing the expressions of the tendency of impulsiveness in matters relating to cloud business and data management security. The significant interaction term indicated that the moderating factor influenced the effect of motor impulsivity on individual behavior's variance and openness to experience, which suggested that the interaction between Big Five personality traits and impulsiveness domains should be centered in business continuity strategies, individual behavior management in cloud business and data security contexts.

Collectively, the findings aligned with a more complex interpretation of cloud security behavior that extends beyond traditional models of rational decision-making. Rather than viewing individuals as purely logical actors who make calculated choices to protect data, the results suggest that human behavior in cloud security is also influenced by emotional, psychological, and personality-related factors. This implied that impulsive tendencies and personal traits can override rational intentions, leading individuals to engage in behaviors that may unintentionally compromise security. The analysis also found disparities in work experience and job titles based on demographic factors. The present study therefore contributes to the understanding of the complex direct associations between motor impulsivity and individual risk

at a behavioral level, which also depend on the indirect effects of personal information privacy concerns and the personality trait of openness to experience. These insights highlight the need for tailored interventions that address both impulsivity and individual personality differences to strengthen cloud security behavior.

Discussion of Results

Motor Impulsivity and Individual Behavior

Motor impulsivity was the only factor that was considered in association with problematic networks, and self-regulation/agreeableness in compliance with cloud business and data security policies (Woods, 2022). The rejection of null hypothesis $H1_0$, that motor impulsivity significantly predicted individual's behavior, was in line with the findings (Alsharida et al., 2023; Aschwanden et al., 2024; McElroy & Dowd, 2023) that identified impulsivity as a significant predictor to risky and noncompliant behavior patterns in different settings including digital environments emphasized the need to address impulsivity tendencies that stains the use of targeted interventions and training programs to improve security measures. For example, Hadlington (2017) administered a questionnaire to investigate the relationship between each of the three subscales of impulsivity (attentional impulsivity, motor impulsivity, and non-planning impulsivity) and risky cybersecurity behaviors. Their findings indicated that both attentional and motor impulsivity were positively correlated with risky behaviors, while non-planning impulsivity was negatively correlated.

Another study by Gillam (2019) contended that motor impulsivity moderated the relationship between disclosure of information and privacy concerns and cybersecurity behavior and suggested future research on the direct impact of motor impulsivity on cybersecurity behaviors. This future research implication aligned with the current study's illustration of motor

impulsivity's significant impact on individual cloud business and data security management behavior. However, the present negative correlation, which indicated the relationship between motor impulsivity and individual behavior in cloud security management, aligned with the available infringes concerning schema impulsivity in cybersecurity implications. To test the generalizability of the overall effect of impulsivity on risky cybersecurity behaviors, a replication study by Aivazpour and Rao (2022) encapsulated the cross-population and cross-setting performances of the same. These results complemented the present study's findings, thus supporting the assumption that impulsive tendencies were the consistent risk factor within a cloud business and digital security setting. Furthermore, the inverse correlation obtained in this study indicated that the higher the level of motor impulsivity, the higher the chances of indulging in activities that breach cloud security measures leading to insider threats. The research goes further than the work of Roberts (2021), which focused on cybersecurity knowledge, attitudes, and online risky behaviors and revealed that, more frequently, behavioral variables suffice over knowledge-based interventions in protecting against online risks.

The core study was dedicated to motor impulsivity and offered a more precise insight into the specific types of impulsive behaviors, such as motor impulsivity, that would influence the result on business operations and data security management. Nevertheless, the correlation between impulsivity and individual behavior was not always the same. AL-Nuaimi (2024) also conducted a systematic review focusing on human and contextual factors affecting cybersecurity in organizations and how individual traits or traits represent different organizational contexts. This contextual difference could be one of the reasons behind some of the finer findings in the present study, which was that the intensity of the quality of motor impulsivity and individual behavior differed between various groups of participants.

Mediating Role of Personal Information Privacy

The mediation role of personal information privacy was statistically significant, given that it explained the individual behavioral process of cloud business and data management security. Personal information privacy is also indirectly linked to motor impulsivity behavior and security, which reflects that the privacy awareness and concern for taking impulsive users are derived from the security behavior. This mediational effect indicated that privacy education and awareness campaigns can be a successful method to mitigate security risk. This mediation effect denoted that privacy education and awareness campaigns can serve as an effective strategy to reduce impulsivity security risk. Thus, the statistical results revealed that personal information privacy not only directly impacted individual behavior but also played a role indirectly through the mediation of motor impulsivity. Since the effect was significant yet did not fully account for the relationship, it indicated partial mediation, meaning that while personal information privacy independently affected individual behavior, motor impulsivity further shaped this relationship. Personal information privacy played a crucial mediating role in the mechanism of motor impulsivity on individual behavior, and this study helped to enrich the behavioral dynamic theory in the field of information security.

Additionally, this study presented the combination of impulsivity construct, information disclosure, and privacy concerns, which depended upon the extent to which business performance affected (Alvazpour and Rao, 2020). Taking stock of such evidence, this research extended prior work by showing that privacy concerns, such as PIP, act as a mediator in the effect of motor impulsivity on personal behavior, specifically with respect to cloud business and data security management. Found that the influence of motivation and privacy on knowledge sharing while sharing information during the pandemic was mediated by perceived risk and

provided evidence of the impact of preconditions relating to privacy on behavioral intentions in cyberspace. This knowledge altered the association between motor impulsivity and self-esteem in the present outcome-driven analysis, which can be traced back to self-interest, personal privacy, and privacy preservation, which were relevant in the study. Soomro et al. (2024) explored digital technology adoption among small and medium-sized enterprises, focusing on the role of privacy implications in adopting technology and technology use patterns. Similarly, Paspatis et al. (2023) contended that personal information privacy concerns are critical factors influencing individual actions directly or indirectly in digital environments. The present research results indicated that security behaviors can only be improved by dealing with both impulsivity management and privacy awareness within organizations. A small part of the mediation implied that although personal information privacy was a key factor, it cannot fully explain the relationship between impulsivity and the behavior associated with cloud business and data management security. Overall, the statistical findings revealed that the criticality of the privacy of personal information to mediate motor impulsivity not only contributed to the academic literature but also bridged the overwhelming concerns regarding business risks and insider threats to data security.

Moderating Effect of Openness to Experience

The significant moderating impact of openness to experience introduced the significance of personality traits in security behavioral pattern design. People who are more open to experience were likely to react differently to impulsive urges in security settings and thus might show more adaptive approaches to security-related situations. The statistical results from this study added to the emerging literature on the personality aspects of business operations and cybersecurity behavior. Srabonee et al. (2025) researched the mechanisms of the influence of

personality dimensions such as Honesty-Humility, Emotionality, Extraversion, Agreeableness, Conscientiousness, and Openness to Experience (HEXACO) on task performance, showing the effect of openness to experience on the patterns of novelty individual behavior. The interaction effect implied that training and intervention programs on security need to be designed based on personalized personality profiles to be as effective as possible. Although there was limited literature concerning how impulsivity impacted decision-making on security issues outside the working environment (Kont, 2023; Shemeis et al., 2021), this study found that openness to experience, one of the Big Five personality traits, played a significant role in shaping individual behavior in cloud business and data security management. Several studies recommended future research on personality traits and their influence on security-related behaviors (Al-Nuaimi et al., 2024; Barth et al., 2019; Chiorri et al., 2016).

Based on the statistical results, the present study found that openness to experience significantly moderated the relationship between motor impulsivity and individual behavior. This statistical finding indicated that the effect of motor impulsivity on individual behavior was influenced by an individual's level of openness to experience. According to Choi et al. (2022), salience was a potential factor within addictive complexity that shapes individuals' capacity to engage in various cloud business and data security behaviors. Meinert et al. (2018) demonstrated that personality significantly influenced various security-related behaviors, including the efficacy of security prompts, susceptibility to phishing attacks, attitudes toward information security, and perceptions of cloud business and data security risks. However, the findings of this study also revealed a negative correlation between motor impulsivity and individual behavior, challenging the positive relationship established by these investigators (Aivazpour & Rao, 2022; Briggs et al., 2017; Hadlington, 2017). Briggs et al. (2017) examined the impact of impulsivity on the

decision-making process in a digital setting and showed that impulsive tendencies can provoke the selection of the least secure options. Contrary to these domains of impulsiveness, they can inhibit the behavior of effectiveness in cloud business and, in essence, from the point of view of heuristic behavior—information security governance, as opposed to reinforcing it. Individualized, behaviorally based methods that include personality temperament and impulsive propensity are much more effective than the one-size-fits-all generic solutions. Interventions like alerts can be modified by organizations to reduce business and security risks. Real-time feedback and phishing simulations. Also, it activated employee vigilance and adherence by role-specific behavioral patterns by means of security training on the security protocols. Models can provide better predictions and interventions by adding the Big Five personality traits and increasing security behavior in the organizational setting.

Integration with Risk Propensity Model

The risk propensity model resurged as a research interest, and its acceptance was renewed due to the recent discovery of its relevance to behavioral constructs, which can be measured through self-reported tools (Zhang et al., 2018). Considering the overall risk propensity model, this study revealed that motor impulsivity influenced individual behavior, personal information privacy mediation, and personality traits, as openness to experience influenced individual behavior. Azizah et al. (2022) compared impulsive buying behavior to factors such as technology acceptance models in e-commerce and showed how impulsivity affected behaviors involving technology intermediaries. Combining the risk propensity model with the factors that affect personality gives an in-depth insight into human behavior in the online space. In the study by Olabanji et al. (2024), cloud security with the use of artificial intelligence (AI) was analyzed, and it was noted that analyzing user behaviors predetermined the results of threat prevention,

showing the crucial necessity to recognize the variations of individual behaviors while implementing security practices.

Recommendations for Future Research

Expansion of Personality Trait Analysis

In future studies, the Big Five personality model should be considered to give a more detailed insight into personality factors reflected in business risk management and cybersecurity behavior. Although, in the current study, the openness to experience variable was pursued, such character traits as conscientiousness, agreeableness, extraversion, and neuroticism could also influence security behaviors. Specifically, conscientiousness can exhibit high positive correlations with security compliance, and neuroticism can affect risk perceptions and security worry. Srabonee et al. (2025) also recommend research into the HEXACO personality model, where an added personality dimension of honesty-humility is added. This characteristic can be of special importance in the cloud and cybersecurity business landscape, where ethical actions and integrity standards are essential to ensure security.

Cross-Cultural and Contextual Studies

Future research must examine the cultural dimensions that may link impulsivity, personality characteristics, and behavior toward security issues. In their article, AL-Nuaimi (2024) focuses on the context of cybersecurity studies and indicates that relationships found in the present study could be significantly moderated by the cultural dimensions (individualism versus collectivism, power distance, and uncertainty avoidance). Inter-industry comparisons also prove instrumental in providing the idea of how the context of organizations affects behavioral relationships. Although the current research was conducted on digital enterprises, some other areas, namely healthcare, government, and educational sectors, can exhibit various streaks due to

different regulations, risk tolerances, and organizational cultures. Future research must also explore the relationships between business and technical job roles and the personality trait differences contributing to cybersecurity behaviors that threaten data security and business losses. Additionally, investigation of role-based training can shed light on enhancing engagement and positive behaviors across all levels.

Longitudinal Behavioral Studies

Longitudinal research designs would contribute to defining causality and determining how the relations between the variables under study could change over time. In those studies, it would be possible to check whether those security training interventions perform the mechanism of changing the effect of impulsivity on security behavior and whether the effect lasts a long time. Moreover, longitudinal research projects may analyze how changes in technology and emergent security threats affect the applicability of personality and behavior-based aspects in online security situations.

Integration of Artificial Intelligence and Behavioral Analytics

Future research must explore how Generative AI and evolving Large Language Models can be leveraged to detect and predict real-time impulsive security behaviors. Olabanji et al. (2024) demonstrated the potential of AI-driven approaches in cloud security, suggesting that behavioral analytics could be combined with personality assessments to develop proactive security interventions. AI integration has potential to optimize cloud business process and security procedures to improve data security. However, future studies must focus on ethical decision-making while applying AI analytics in practice. Overall, organizational cultural sensitivity investigation need attention to enrich academic scholarship.

Practical Implications

Personalized Security Training Programs

The study results have important implications for designing the training sessions based on individual personality differences (impulsivity and openness to experience). High-motor impulsivity employees could benefit from learning self-regulation skills, mindfulness skills, and decision-making procedures. To increase interest and understanding, training programs should include interactive content, simulations that apply in the real world, and personal responses to increase interaction. The outstanding play of individual information privacy as a mediator implies that privacy awareness training is to be combined with the programs of impulsivity management to gain the most efficiency.

Organizations should introduce well-calculated behavioral intervention plans that deal with impulsive trends before they culminate in security infringements. Such solutions involve live behavioral notifications, auto information of risks, and involuntary recession times of high-security decisions. The prescriptive measures that continuously assist impulsive employees are the mentorship programs between impulsive and security-minded colleagues. Repeated behavior tests and personal feedback may assist employees in creating higher levels of self-recognition and self-control. This research promoted the development of practical security guidance, training, and policy enforcement tailored to the specific job roles to reduce human errors and protect business security. The researcher proposed a simple questionnaire to serve as a structured tool to evaluate the impulsive tendencies of the employees without requiring complex behavioral assessments:

1. Do you take a decision ready made by you or somebody instantaneously?
2. How often at work do you take a risk without paying heed to the consequences?

3. Are you constantly jumping from one task to another? How do you respond to a problem?
4. Do you deal with it immediately or do you think about it?
5. Do you focus more on short-term results than long-term goals?

Organizations can integrate the above questions in evaluating employee behaviors to phishing simulations to track patterns in impulsive decision-making and adjust security protocols accordingly. Furthermore, human resource administrations can use these questions to identify impulsive candidates, and the insights will help them make appropriate decisions to benefit the business's performance.

Data Security Culture

The results reveal the essence of building organizational security cultures, considering individual personality and behavioral differences. Organizations must abolish the one-size-fits-all security policies and introduce fluid frameworks to fit the various personality types and behavioral patterns. Training managers and security professionals about personality awareness should be one of the sections of security culture practice so that they know how to take care of individual disparities in security behavior. Periodic testing of culture is beneficial because organizations can tell where personality issues are causing security weaknesses.

Integration of Technology and User Experience Design

Security technologies must also be creative, considering that personality characteristics and impulsivity can affect user interactions. Security system user interfaces must also contain behavioral nudges and decision support applications that lead impulsive users to make more considered security choices. Adaptable security systems that will change their demands and cues according to the profiles of particular individuals may improve security effectiveness and user

satisfaction. These systems would be a significant step towards the security of human-centered designs.

Theoretical Implications

Risk Propensity Model Enhancement

The results from the study were helpful in further elaborating and enhancing the model of risk propensity in the context of cybersecurity. The finding of motor impulsivity as a contributing factor in predicting individual behavior in cloud business and data security management is empirical evidence that should be supported by including personality traits in the current theories. Such integration is in conjunction with the shortcomings of the traditional models used in the rational choice that suggest a homogeneous decision-making process. The partial mediation effect of personal information privacy implies that the current models need to include the various mechanisms of pathways to explain the behavioral outcomes. The interplay between personality and environmental dimensions, as well as cognitive processes, should be viewed in terms of how these interact to influence security behavior in the future, as far as theoretical development is concerned.

By showing the relevance of individual differences when making decisions concerning security, this study adds to the research on behavioral security, an area increasingly gaining intellectual attention. The fact that openness to the experience provided a strong moderating effect undermines the idea of the uniformity of reactions to security training and interventions. It helps to develop more complex theoretical frameworks. The results show that it is possible to refer to personality psychology, combining it with the theory of information security, opening up possibilities for the interdisciplinary development of theories. Such intertwining might increase

the number of predictive models for mitigating business risks, improving security behavior, and more efficient forms of intervention.

Implications for Technology Acceptance Models

The findings from this study also have important implications for technology acceptance models in cloud business and online data security landscapes. The fact that personality traits (e.g., openness to experience) interact with motor, the relationship between impulsivity and individual behavior, suggests that technology acceptance models should be expanded to include impulsivity and individual difference variables in order to extend their predictive capabilities and validity. This interaction of impulsivity and a security technology acceptance perspective suggests that conventional theorizing has limitations when considering behavior in high-stakes security contexts, as emotions and impulsive responses may override rational decision-making.

Limitations of the Study

Self-Report Measurement Limitations

The use of self-reported measures in the study poses the risk of having possible biases that can invalidate the study results. Social desirability bias could have occurred in a way that participants underreported the tendency to perform impulsively or overreported that tendency to security consciousness. Furthermore, the self-report of the measures of the personality traits may not address the richness of behavioral entries within real-life protection environments. Behavioral response variations were due to changes in security threats, organizational policies, or circumstances. Sparse literature may lead to overlooked confounding factors or alternative explanations. Future studies need to or should integrate behavioral observation, physiological measures, or experimental manipulation that will authorize the conclusions made on self-report and give more objective determinations of the correlations of variables in the study.

Generalizability Constraints

The study's limitations lay in the relevance of research outcomes to other forms of organizations and cultural environments since the study focuses on digital enterprises in particular geographical and cultural locations. Some relationships between personality traits and security behavior may differ in industries, organizational cultures, and even the national context. The generalizability of findings can also be affected by the nature of the sample, including the demographic distributions and managerial roles. Future studies should evaluate the relationships using various populations and settings to determine generalizability.

Time and Causal Restrictions

The study was cross-sectional. Thus, it does not allow for determining causal relationships among variables. Although the proposed directional relationships rely on a theoretical rationale, longitudinal studies would bring more evidence of causality. The study also does not consider temporal behavior variations due to changes in security threats, organizational policies, or circumstances. The relationships identified during the study might change depending on these dynamic factors.

Measurement Scope Limitations

The researcher synthesized and interpreted the key findings of this research, focusing on the relationships between motor impulsivity(predictor), personal information privacy (mediator), openness to experience (moderator), and individual behavior (criterion) in cloud security management. However, the study focused primarily on specific aspects of motor impulsivity, openness to experience as one of the personality traits, and individual security behavior, which may not capture the full range of relevant variables in cybersecurity contexts. Personality traits, cognitive factors, and environmental variables may also be essential in determining security

behavior. The outcome of individual behavior cannot be fully represented through self-reported scales, and comprehensive behavioral construct assessments would rather provide enriched descriptive insights into the practical implications.

Summary. The research findings on the effect of motor impulsivity on cloud security individual behavior in digital enterprises that were analyzed comprehensively appear in Chapter Five. The statistical results confirmed the key relationships in all the hypotheses tested: that motor impulsivity negatively influenced individual behavior, personal information privacy partially moderated this relationship, and openness to experience significantly mediated the influence of motor impulsivity on individual behavior. Interpretation of results puts these findings into the perspective of the literature in the field, pointing out similarities and exceptional contributions to the field of study. The study results correspond to well-developed research directions on impulsivity in cybersecurity and introduce new information on mediating and moderating processes that shape the connection between variables.

Future research recommendations are related to the increased analysis of personality traits, cross-cultural research, longitudinal studies, and the incorporation of AI methods. These suggestions serve as precise guidelines on how to make achievements in the conduct of studies regarding behavioral cybersecurity. The practical implications of the study rest on the emphasis on the need to design individual security interventions, adopt approaches to behavioral management, and promote individual-based security cultures in organizations. These implications give practical directions to organizations to improve their effectiveness in protecting themselves from business risks and data breaches using human-oriented initiatives. The theoretical implications contribute to the advancement of behavioral security theory by presenting the significance of personality factors to the security-related decision-making process

and the justification to integrate behavioral and technology acceptance theories with information security-related frameworks.

Conclusion

This study was insightful regarding complicated issues between motor impulsivity, openness to experience personality traits, and individual behavior in digital businesses and data security management. The outstanding results of all hypotheses prove that the variability of individuals is essential in shaping patterns of cybersecurity behavior. The inverse motor impulsivity security behavior, the incomplete mediating effect of personal information privacy, and the facilitating moderating effect of openness to experience in valuing the division into behavioral dimensions consideration in cloud business and data security management.

The research implications are not limited to academic learning. Instead, it will be used in practice in organizations' security management. The results allow for building individual security solutions based on the differences in personality and behavior. This knowledge can enable organizations to develop more efficient training, specific behavioral interventions, and security cultures related to different personality types. The study findings were another gateway to control insider threats, eventually improving business performance and steering towards a data-driven culture. The theoretical implications of the research are to build knowledge in behavioral security involving the combination of personality and information security theory. Such integration enables a starting point for framing more advanced security behavior models to anticipate and describe individual variations in security-related decision-making accurately.

The practical implications insist on the necessity of organizations to shift away from blind, standard patterns in the formulation of the means of securing their organizations to be more distant, personality-based solutions. Creating assessment tools, personal training programs,

and adaptive security systems are all significant opportunities for better organizational security postures. These findings require follow-up studies in the future in terms of expanding the domain of analysis of personality traits, the cross-cultural study, the use of long-term research, and the quest to integrate artificial intelligence into behavioral security. These research areas will also help to gain better insights into the role of human factors in cybersecurity and help develop more successful security management practices.

A commitment to study limitations helped to give insight into the range and limitations of the findings, and the conclusion is analyzed to render the most important contributions and significance to business continuity, mitigate data breaches, and practice cybersecurity management. The discussion in the chapter illustrated that getting into the particularities of individual differences in personality and behavior was key to avoiding business risks and productive cybersecurity management in modern digital enterprises. Possible conclusions that can be drawn about this study were the significance of managing motor impulsivity in security education and treatment, the usefulness of integrating the privacy awareness component in business strategies, security behavioral treatment programs, and the importance of developing security strategies that are differentiated according to the personality characteristics of individuals. The insights are valuable insights into how human factors work and how they can be controlled in the cybersecurity business, as well as both theory and practice about the effectiveness of an organization's security.

References

Adjorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. *Canadian Review of Sociology, 56*(1), 8-29. https://doi.org/10.1111/cars.12227

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Farheen, Z. (2019). Qualitative v/s. Quantitative research-A- A summarized review. *Population*, *1*(2). doi:10.18410/jebmh/2019/587

Ahmadi, S. (2024) Systematic literature review on cloud computing security: Threats and mitigation dtrategies, *Journal of Information Security*, *15*, 148-167. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9404177

Ahmed, A. M., Bello, A., Maurushat, A., & Moustafa, A. (2021). The role of user behavior in improving cyber security management. *Frontiers in Psychology*, *12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Aiken, M. (2016). The cyber effect: *A pioneering cyber-psychologist explains how human behavior changes online*. Spiegel & Grau. https://static10.labirint.ru/books/741057/demo.pdf

Aivazpour, Z., & Rao, V. S. (2020). Information disclosure and privacy paradox: The role of impulsivity. *ACM SIGMIS Database, 51*(1), 14-36. https://doi.org/10.1145/3380799.3380803

Aivazpour, Z., & Rao, C. (2022). A replication study of the impact of impulsivity on risky cybersecurity behaviors. *AIS Transactions on Replication Research, 8*(1), *3.* https://doi.org/10.17705/1atrr.00074

Akeiber, H. J. (2025). The evolution of social engineering attacks: A cybersecurity engineering perspective. *Al-Rafidain Journal of Engineering Sciences*, *3*(1), 294-316. https://doi.org/10.61268/r9c49865

Alashoor, T., Keil, M., Smith, J., & McConnell, A. R. (2022). Too tired and in too good of a mood to worry about privacy: Explaining the privacy paradox through the lens of effort levels in information processing. *Information Systems Research, 34*(4), 1415-1436. https://doi.org/10.1287/isre.2022.1182

Alenizi , J. & Alrashdi, I. (2023). SFMR-SH: Secure framework for mitigating ransomware attacks in smart healthcare using blockchain technology. *Sustainable Machine Intelligence Journal*, *2*(4), 1–19. doi:10.18410/jebmh/2019/5

Ali, M., Lei, S., & Wei, X. Y. (2018). The mediating role of the employee relations climate in the relationship between strategic HRM and organizational performance in Chinese banks. *Journal of Innovation and Knowledge*, *3*(3), 115–122. https://doi.org/10.1016/j.jik.2016.12.003

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, *13*(9), 5700. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9404177

AL-Nuaimi, M. N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: A systematic review. *Global Knowledge, Memory and Communication*, *73*(1/2), 1-23. https://doi.org/10.1108/GKMC-12-2021-0209

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*. https://doi:10.1016/j.techsoc.2023.102258

Alrashdi, A. S. (2023). *The Influence of users' addictive behaviors on the relationships between information security countermeasures and risky cybersecurity practices* (Publication No. 2843040280) [Doctoral dissertation, British University]. ProQuest Dissertations & Theses Global.

Alvazpour, Z., & Rao, A. (2022). Revisiting the correlates of impulsivity and risky cybersecurity behaviors: A replication study. *Computers & Security*, *110*, 102449. https://doi.org/10.1016/j.cose.2022.102449

Alves, M.M. (2023). What is cloud computing?. In: Borin, E., Drummond, L.M.A., Gaudiot, JL., Melo, A., Melo Alves, M., Navaux, P.O.A. (eds) *High performance computing in clouds* . Springer, Cham. https://doi.org/10.1007/978-3-031-29769-4_2

Ana, L. (2024). *A research study of employee perceptions on identifying phishing attacks in financial organizations* (Publication No. 3056586847) [Doctoral dissertation, University of South Carolina]. ProQuest Dissertations & Theses Global.

Anastasiei, B., Voda, A. I., Florea, N., Costuleanu, C. L., & Clipa, C.-I. (2020). Measuring the Big Five personality traits effects on manager's propensity to take risks. *Transformations in Business & Economics, 19*(2B), 944-959. https://openurl.ebsco.com/EPDB%3Agcd%3A12%3A7879596/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A147236772&crl=c&link_origin=scholar.google.com

Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behavior: The psychological gateway for cyberattacks. *Organizational Cybersecurity Journal: Practice, Process & People*, *4*(1), 32–50. https://doi.org/10.1108/OCJ-02-2023-0004

Aspelmeier, J. (2005) *Table of critical values for Pearson's r*. https://pdf4pro.com/amp/view/table-of-critical-values-for-pearson-s-r-59198f.html

Aivazpour, Z., & Rao, C. (2022). A replication study of the impact of impulsivity on risky cybersecurity behaviors. *AIS Transactions on Replication Research*, *8*(1), 3. https://doi.org/10.17705/1atrr.00074

Azizah, F. D., Nur, A. N., & Putra, A. H. P. K. (2022). Impulsive buying behavior: Implementing IT on technology acceptance model on e-commerce purchase decisions. *Golden Ratio of Marketing and Applied Psychology of Business*, *2*(1), 58-72. https://goldenratio.id/index.php/grmapb/article/view/173

Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, 31, 12. https://doi.org/10.1177/03128962241293658

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics, 41,* 55-69. https://doi.org/10.1016/j.tele.2019.03.003

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 1017–1041. https://doi.org/10.2307/41409971

Bureau of Labor Statistics. (2023). *Healthcare occupations: Characteristics of the employed. U.S. Department of Labor*. https://www.bls.gov/ooh/healthcare/

Blevins, D. P., Stackhouse, M. R. D., & Dionne, S. D. (2021). Righting the balance: Understanding introverts (and extraverts) in the workplace. *International Journal of Management Reviews, 24*(1), 78-98. https://doi.org/10.1111/ijmr.12268

Bradley, T. (2024). Splunk report highlights the cost of human error. https://www.forbes.com/sites/tonybradley/2024/06/26/splunk-report-highlights-the-cost-of-human-error/

Brown, T. (2025). *Impact of data security breach on long-term firm performan*ce (Order No. 31933800). Available from ProQuest Dissertations & Theses Global. (3203060758). https://links.franklin.edu/login?url=https://www.proquest.com/dissertations-theses/impact-data-security-breach-on-long-term-firm/docview/3203060758/se-2

Briggs, P., Jeske, D., & Coventry, L. (2017). *Behavior change interventions for cybersecurity. In L. Little, E. Sillence, & A. Joinson (Eds.), Behavior change research and theory: Psychological and technological perspectives* (pp. 115–136). https://doi.org/10.1016/B978-0-12-802690-8.00004-9

Blaschke, M. (2019). Socio-technical complexity in digital platforms: The revelatory case of *Helix Nebula*: *The Science Cloud*. In: Urbach, N., Röglinger, M. (eds) Digitalization Cases. Management for Professionals. Springer, Cham. https://doi.org/10.1007/978-3-319-95273-4_9

Bolek, V., & Romanová, A. (2020). Predictors of ambient intelligence: An empirical study in enterprises in Slovakia. *Electronics*, *9*(10), 1655. https://doi.org/10.3390/electronics9101655

Bucea-Manea-Țoniş, R., Prokop, V., Ilic, D., Gurgu, E., Bucea-Manea-Țoniş, R., Braicu, C., & Moanță, A. (2021). The relationship between eco-innovation and smart working as support for sustainable management. *Sustainability*, *13*(3), 1437. https://doi.org/10.3390/su13031437

Buelow, M. T., & Cayton, C. (2020). Relationships between the big five personality characteristics and performance on behavioral decision-making tasks. *Personality and Individual Differences, 160,* 109931. https://doi.org/10.1016/j.paid.2020.109931

Burt, A. (2019, January 3). Privacy and cybersecurity are converging. Here's why that matters for people and companies. https://www.investkl.gov.my/clients/asset_28B5D799-69B3-4BCB-B61B-D284619547A3/uploads/Privacy-and-Cybersecurity-Are-Converging.PDF

Burton, S.L., Burrell, D.N., Nobles, C., & Jones, L.A.(2023). Exploring the nexus of cybersecurity leadership, human factors, emotional intelligence, innovative work behavior, and critical leadership traits. *Science Bulletin*, *28*(2), 162–175. https://doi.org/10.2478/bsaft-2023-0016

Caci, B., Cardaci, M., & Miceli, S. (2019). *Development and maintenance of self-disclosure on Facebook: The role of personality traits*. *SAGE Open.* https://doi.org/10.1177/2158244019856948

Cadwell, R. (2023, April 27). *Average Cost of a Data Breach.* https://phoenixnap.com/blog/cost-of-data-breach

Campisi, T., Severino, A., Al-Rashid, M. A., & Pau, G. (2021). The development of the smart cities in the connected and autonomous vehicles (CAVs) Era: From mobility patterns to scaling in cities. *Infrastructures*, *6*(7), 100. https://doi.org/10.3390/infrastructures6070100

Carden, J., Jones, R. J., & Passmore, J. (2021). Defining self-awareness in the context of adult development: A systematic literature review. *Journal of Management Education, 46*(1). https://doi.org/10.1177/1052562921990065

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior, 69*, 207–217. doi.org/10.1016/j.chb.2016.12.013

Chiorri, C., Marsh, H. W., Ubbiali, A., & Donati, D. (2016). Testing the factor structure and measurement invariance across gender of the Big Five Inventory through exploratory structural equation modeling. *Journal of Personality Assessment*, *98*(1), 88–99. https://doi.org/10.1080/00223891.2015.1035381

Choi, H. S., Carpenter, D., & Ko, M. S. (2022). Risk-taking behaviors using public Wi-fi™. *Information Systems Frontiers*, 1-18. https://doi.org/10.1007/s10796-021-10119-7

Collier, B. (2023). *Considerations for selecting and implementing cloud business and data security solutions using cloud access security brokers* (Publication No. 2807030349) [Doctoral dissertation, Marymount University]. ProQuest Dissertations & Theses Global.

Clifton, A. (2024). *Strategies for insider threat mitigation and detectio*n (Publication No. 2807030349) [Doctoral dissertation, Walden University]. ProQuest Dissertations & Theses Global.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., & Huettel, S. (2014). An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale. *Archives of Scientific Psychology*, *2*(1), 1–12. doi: 10.1037/arc0000005

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. https://doi.org/10.22215/timreview/835

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Cui, G., Wang, F. & Zhang, Y. (2023). Buffer or boost? the role of openness to experience and knowledge sharing in the relationship between team cognitive diversity and members' innovative work behavior. *Current Psychology*, *42*, 25233–25245. https://doi.org/10.1007/s12144-022-03633-7

Cybersecurity & Infrastructure Security Agency (CISA). (2025). *Phishing attacks: Prevention and mitigation strategies*. U.S. Department of Homeland Security. https://www.definitions.net/definition/phishing

Dalal, R. S., & Gorab, A. K. (2016). *Insider threat in cybersecurity: What the organizational psychology literature on counterproductive work behavior can and cannot (yet) tell us. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), Psychosocial dynamics of cybersecurity* (pp. 92–110). Routledge/Taylor & Francis Group.

Dalimarta, F., Andono, P. N., Soeleman, M. A., & Hasibuan, Z. A. (2025). Towards automated motor impulsivity monitoring in real-world scenarios: A multiple object tracking approach. *Data Science: Journal of Computing and Applied Informatics*, *9*(1), 1–17. https://doi.org/10.32734/jocai.v9.i1-16686

Dash, G. F., Slutske, W. S., Martin, N. G., Statham, D. J., Agrawal, A., & Lynskey, M. T. (2019). Big Five personality traits and alcohol, nicotine, cannabis, and gambling disorder

comorbidity. *Psychology of Addictive Behaviors, 33*(4), 420-429. https://doi.org/10.1037/adb0000468

Demaree, H. A., Everhart, D. E., Youngstrom, E. A., & Harrison, D. W. (2005). Brain lateralization of emotional processing: Historical roots and a future incorporating "dominance." *Behavioral and Cognitive Neuroscience Reviews*, *4*(1), 3–20. https://doi.org/10.1177/1534582305276837

Demircioglu, Z. I., & Kose, A. G. (2022). Mediating roles of impulsivity and risk-taking in the links of the dark triad traits with flirting and dating via social media. *Studies in Psychology, 42*(3), 643-685. http://doi.org/10.26650/SP2021-1018862

de Paula, J. J., Costa, D. d. S., de Miranda, D. M., & Romano-Silva, M. A. (2020). The abbreviated version of the Barratt Impulsiveness Scale (ABIS): Psychometric analysis, reliable change indexes in clinical practice and normative data. *Psychiatry Research*, *291*. https://doi.org/10.1016/j.psychres.2020.113120

de Souza, R. (2025). EU: DLA Piper GDPR fines and data breach survey. https://privacymatters.dlapiper.com/2025/01/eu-dla-piper-gdpr-fines-and-data-breach-survey-january-2025/

Dezhkam, N., Bahri, M. R. Z., & Keshi, A. K. (2022). The effect of impulsivity on addiction and addictive tendencies: A meta-analysis. *Journal of Health Reports and Technology, 8*(3), e120846. https://doi.org/10.5812/jhrt-120846

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.1365-2575.2006.00220.x

Ding, J., Qian, P., Ma, J., Wang, Z., Lu, Y., & Xie, X. (2024). Detect insider threat with associated session graph. *Electronics, 13*(24), 4885. https://doi.org/10.3390/electronics13244885

Diotaiuti, P., Mancone, S., Corrado, S., de Risio, A., Cavicchiolo, E., Girelli, L., & Chirico, A. (2022). *Cloud addiction in young adults: The role of impulsivity and codependency*. https://www.frontiersin.org/articles/10.3389/fpsyt.2022.893861/full**X**

Dornheim, P., & Zarnekow, R. (2024). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information Computer Security*, *32*(2), 179–196. https://doi.org/10.1108/ICS-07-2023-0116

Dogruel, L., Joeckel, S., & Vitak, J. (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior*, *77*, 230–239. https://doi.org/10.1016/j.chb.2017.08.035

Durodolu, O. O. (2016). Technology acceptance model as a predictor of using information system to acquire information literacy skills. *Library Philosophy and Practice (e-journal)*, *12(2), 1450*. https://digitalcommons.unl.edu/libphilprac/1450

Edwards, M. A., Howcroft, J. G., & Lambert, T. (2021). Young adults' perceptions of online self-disclosure. *Review of European Studies, 13*, 26-26. https://doi.org/10.5539/res.v13n1p26

Evans, H. (2018). *The influence of personality traits and ict use on the boundary management of home-based teleworkers* (Publication No. 2116914989) [Doctoral dissertation, Loughborough University]. ProQuest Dissertations & Theses Global.

Ewan, P. E. (2024). Cybersecurity *Framework for Assessing the Efficiency of AI-Based Intrusion Detection Cybersecurity Techniques* (Publication No. 3070484019) [Doctoral dissertation, National University]. ProQuest Dissertations & Theses Global.

Faro, C. (2023, November 22). *Kaspersky's research confirms that information security violations by staff are almost equally as common as cybersecurity breaches*. Usa.Kaspersky.com. https://usa.kaspersky.com/about/press-releases/kaspersky-research-confirms-information-security-violations-by-staff-are-almost-equally-as-common-as-cybersecurity-breaches

Faschang, T., Macher, G., & Veledar, O. (2024). A comprehensive training approach for automotive cybersecurity engineering. *SAE Technical Paper,* 01-2800. https://doi.org/10.4271/2024-01-2800

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*, 1149-1160.https://doi.org/10.3758/BRM.41.4.1149

Fenton-O'Creevy, M., & Furnham, A. (2019). Money attitudes, personality and chronic impulse buying. *Applied Psychology, 69*(4). https://doi.org/10.1111/apps.12215

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & security*, *59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Franklin University. (2025). *Institutional Review Board*. https://www.franklin.edu/about-us/policy-information/institutional-review-board

Frauenstein, E. D. (2021). *A personality-based behavioral model: Susceptibility to phishing on social networking sites.* https://doi.org/10.21504/10962/190306

Gallegos, J., Arévalo, P., Montaleza, C., & Jurado, F. (2024). Sustainable electrification—advances and challenges in electrical-distribution networks: A Review. *Sustainability*, *16*(2), 698. https://doi.org/10.3390/su16020698

Garcia, D., Cloninger, K. M., & Cloninger, C. R. (2023). Coherence of character and temperament drives personality change toward well-being in person-centered therapy. *Current Opinions in Psychiatry, 36*(1), 60-66. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9794122/

Garcia-Argibay, M. (2019). The relationship between the Big Five personality traits, impulsivity, and anabolic steroid use. *Substance Use & Misuse 54*(2), 236-246. https://doi.org/10.1080/10826084.2018.1512630

Georgiadou, A.,Mouzakitis, S., Bounas, & K., Askounis, D. (2022). A cyber security culture framework for assessing organization readiness. J*ournal of Computer Information Security*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Gillam, A. R. (2019). Technology threat avoidance factors as predictors of risky cybersecurity behavior within the enterprise (Publication No. 2239996649) [Doctoral dissertation, Indiana State University]. ProQuest Dissertations & Theses Global.

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behaviors, 108,* 106319. https://doi.org/10.1016/j.chb.2020.106319

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cybersecurity behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Goel, S., Williams, K., Huang, J., & Dennis, A. (2019). Does privacy mean different things to different people: Can that explain the privacy paradox? *WISP 2019* Proceedings*, 2.* https://aisel.aisnet.org/wisp2019/2/

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in Personality, 37*(6), 504–528. https://doi.org/10.1016/S0092-6566(03)00046-1

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: impact of generative AI in cybersecurity and privacy. *IEEE Access, 11,* 80218-80245. https://doi.org/10.1109/ACCESS.2023.3300381

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society, 50,* 101660. https://doi.org/10.1016/j.scs.2019.101660

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Havrilko, V. R. (2016). *Internet addiction and repeat purchase intention: Exploring the moderating effects of brand trust, neuroticism, risk aversion, post purchase regret and intrinsic motivation* (Publication No. 1854134521) [Doctoral dissertation, Trident University International]. ProQuest Dissertations & Theses Global.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. The Guilford Press.

Hayes, A. F., & Scharkow, M. (2013). The relative trustworthiness of inferential tests of the indirect effect in statistical mediation analysis: Does method really matter? *Psychological Science, 24* (10), 1918–1927. https://doi.org/10.1177/0956797613480187

Heinström, J., Nikou, S., & Sormunen, E. (2022). Hide and seek—the role of personality, sense of coherence and experiential information in hidden information needs. *Journal of Documentation, 78*(4), 780-799. https://doi.org/10.1108/JD-06-2021-0124

Highhouse, S., Wang, Y., & Zhang, D. C. (2022). Was risk propensity unique from the big five factors of personality? A meta-analytic investigation. *Journal of Research in Personality, 98,* 104206. https://doi.org/10.1016/j.jrp.2022.104206

Hirschprung, R. S., Klein, M., & Maimon, O. (2022). Harnessing soft logic to represent the privacy paradox. *Informatics, 9*(3), 54. https://doi.org/10.3390/informatics9030054

Hogan, R., & Sherman, R. A. (2020). Personality theory and the nature of human nature. *Personality and Individual Differences, 152,* 109561. https://doi.org/10.1016/j.paid.2019.109561

Horwood, S., & Anglim, J. (2021). Emotion regulation difficulties, personality, and problematic smartphone use. *Cyberpsychology, Behavior, and Social Networking, 24*(4). https://doi.org/10.1089/cyber.2020.0328

Hwang, S. (2024). Towards End-to-End Data Privacy: From Generation to Consumption (Publication No. 3088124331) [Doctoral dissertation, University of California]. ProQuest Dissertations & Theses Global.

IBM. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

IBM. (2025). *What was phishing*? https://www.ibm.com/think/topics/phishing

Indrajaya, A. N. (2022). The effect of Big Five Model (BFM) personality traits on online impulsive buying: Evidence from website user in DKI Jakarta area. *International Journal of Business, Economics and Law, 26*(1), 108-120. https://ijbel.com/wp-content/uploads/2022/03/IJBEL26.ISU1_226.pdf

International Organization for Standardization. (2013). Information technology — security techniques — information security management systems — requirements (ISO/IEC 27001:2013). https://www.iso.org/standard/54534.html

Ioannou, A., Tussyadiah, I., & Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing, 38*(10), 1766-1778. https://doi.org/10.1002/mar.215229

ISO & IEC. (2022). *ISO/IEC 27001:2022 Information security management systems—Requirements*. https://www.iso.org/standard/27001

Jamieson, M. K., Govaart, G. H., & Pownall, M. (2023). Reflexivity in quantitative research: A rationale and beginner's guide. *Social and Personality Psychology Compass*, *17*(4), e12735. https://doi.org/10.1111/spc3.12735

Jawinski, P., Markett, S., Sander, C., Huang, J., Ulke, C., Hegerl, U., & Hensch, T. (2021). The Big Five personality traits and brain arousal. *Brian Science, 11*(10), 1272. https://doi.org/10.3390/brainsci11101272

Jeske, D., Briggs, P., & Coventry, L. (2016). Exploring the relationship between impulsivity and decision-making on mobile devices. *Personal and Ubiquitous Computing*, 20, 545-557. https://doi.org/10.1007/s00779-016-0938-4

Ji, T. (2022). *Data Security and Privacy under the Binary Cloak* [Doctoral dissertation, Case Western Reserve University]. OhioLINK Electronic Theses and Dissertations Center. http://rave.ohiolink.edu/etdc/view?acc_num=case1654694966399779

Jochemczyk, L., Pietrzak, J., Buczkowski, R., Stolrski, M., & Markiewicz, L. (2017). You only live once: Present-hedonistic time perspective predicts risk propensity. *Personality and Individual Differences, 115,* 148-153. https://doi.org/10.1016/j.paid.2016.03.010

Johnson, C. E. (2024). *Big Five Personality Traits and Perceived Job Stress Among K-12 Special Education Teachers* (Publication No. 3078873940) [Doctoral dissertation, Grand Canyon University]. ProQuest Dissertations & Theses Global.

John, O. P., & Srivastava, S. (1999). *The Big Five Trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), Handbook of personality: Theory and research (2nd ed., pp. 102–138).* Guilford Press.

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information and Computer Security, 31*(4), 463-477. https://doi.org/10.1108/ICS-08-2022-0139

Kang, H. (2013). A guide on the use of factor analysis in the assessment of construct validity. *Journal of Korean Academy of Nursing*, *43*(5), 587–594. https://koreascience.kr/article/JAKO201304962315783.page

Khadka, K., & Ullah, A.B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*, 119. https://doi.org/10.1007/s10207-025-01032-0

Kahil, B. (2021). Motivation and privacy role in knowledge sharing during pandemic 2020: A study of enterprise social system use in Malaysian SMEs. *Journal of Digitization and Information System*, *1*(1), 28-42. https://doi.org/10.54433/JDIIS.2021100003

Khan, D., Arjmandi, M. K., & Yuvaraj, M. (2021). Most Cited Works on Cloud Computing: The 'Citation Classics' as Viewed through Dimensions.ai. *Science & Technology Libraries*, *41*(1), 42–55. https://doi.org/10.1080/0194262X.2021.1951424

Khan, H.U., Khan, R.A., & Alwageed, H.S. (2025). AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm. *Science Reports*, *15*(1), 13423. https://doi.org/10.1038/s41598-025-97204-y

Kiire, S., Matsumoto, N., & Yoshido, E. (2020). Discrimination of Darl Triad traits using the UPPS-P model of impulsivity. *Personality and Individual Differences, 167,* 110256. https://doi.org/10.1016/j.paid.2020.110256

Kont, K. (2023). Libraries and cyber security: the importance of the human factor in preventing cyber-attacks. *Library Hi Tech News*, *41*(1), 11–15. https://doi.org/10.1108/LHTN-03-2023-0036

Kowalski, C. M., Vernon, P. A., & Schermer, J. A. (2021). The dark triad and facets of personality. *Current Psychology, 40,* 5547-5558. https://doi.org/10.1007/s12144-019-00518-0

Kreibich, A., Hennecke, M., & Brandstätter, V. (2020). The effect of self-awareness on the identification of goal-related obstacles. *European Journal of Personality, 34*(2). https://doi.org/10.1002/per.2234

Kreibich, A., Wolf, B. M., Bettschart, M., Ghassemi, M., Herrmann, M., & Brandstätter, V. (2022). How self-awareness was connected to less experience of action crises in personal

goal pursuits. *Motivation and Emotion, 46,* 825-836. https://doi.org//10.1007/s11031-022-09942-5

Kshetri, N. (2017). Blockchain's role in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kun, B., Takacs, Z. K., Richman, M. J., Griffiths, M. D., & Demetrovics, Z. (2021). Work addiction and personality: A meta-analytic study. *Journal of Behavioral Addictions, 9*(4), 945-966. https://doi.org/10.1556/2006.2020.00097

Le, N. T. (2019). *A Novel Capability Maturity Model with Quantitative Metrics for Securing Cloud Computing* (Publication No. 10169573) [Doctoral dissertation, Wilmington University of Technology Sydney]. ProQuest Dissertations & Theses Global.

Lee, S. D., Kuncel, N. R., & Gau, J. (2020). Personality, attitude, and demographic correlates of academic dishonesty: A meta-analysis. *Psychological Bulletin, 146*(11), 1042-1058. https://doi.org/10.1037/bul0000300

Lembcke, T.-B., Engelbrecht, N., Brendel, A. B., & Kolbe, L. M. (2019). *To nudge or not to nudge: Ethical considerations of digital nudging based on its behavioral economics roots*. Proceedings of the European Conference on Information Systems. https://www.researchgate.net/publication/333421600_To_Nudge_or_Not_To_Nudge_Ethical_Considerations_of_Digital_Nudging_Based_on_Its_Behavioral_Economics_Roots

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7,* 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li., L., Chen, Y., & Liu, Z. (2022). Shyness and self-disclosure among college students: The mediating role of psychological security and its gender difference. *Current Psychology, 41,* 6000-6013. https://doi.org/10.1007/s12144-020-01099-z

Lin, C., Song, Z., Song, H., Zhou, Y., Wang, Y., & Wu, G. (2016). Differential privacy preserving in big data analytics for connected health. *Journal of medical systems*, *40*, 1–9. https://link.springer.com/article/10.1007/s10916-016-0446-0

Luo, X., Ge, Y., & Qu, W. (2023). The association between the Big Five personality traits and driving behaviors: A systematic review and meta-analysis. *Accident Analysis, 183,* 106968. https://doi.org/10.1016/j.oop.2023.106968

Lv, Y., Fang, G., Zhang, X., Wang, Y., & Wang, Y. (2022). Influence of personality traits on online self-disclosure: Considering perceived value and degree of authenticity separately as mediator and moderator. *Frontiers in Psychology, 13.* https://doi.org/10.3389/fpsyg.2022.958991

Lyvers, M., Senturk, C., & Thorberg, F. A. (2021). Alexithymia, impulsivity and negative mood in relation to cloud addiction symptoms in female university students. *Australian Journal of Psychology, 73*(4), 548-556. https://doi.org/10.1080/00049530.2021.1942985

Malesza, M. (2020). The effects of Dark Triad traits in a prisoner's dilemma game. *Current Psychology, 39.* https://doi.org/10.1007/s12144-018-9823-9

Malesza, M., & Kalinowski, K. (2021). Willingness to share, impulsivity and the Dark Triad traits. *Current Psychology, 40,* 3888-3896. https://doi.org/10.1007/s12144-019-00351-5

Mangera, R. (2019). *The Dark triad, sensation-seeking and impulsivity in young South African adults.* UPSpace. https://repository.up.ac.za/handle/2263/72789

Mantilla, E., & Robles-Flores, J. A. (2021). *The role of risk aversion in the privacy paradox on Cloud users*. https://web.archive.org/web/20220802073544id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1358&context=amcis2021

Mazurczyk, W., Bisson, P., Jover, P. R., Nakao, K., & Cabaj, K. (2020). Challenging and novel solutions for 5G network security, privacy and trust. *IEEE Wireless Communications, 27*(4). https://doi.org/10.1109/MWC.2020.9170261

McClain, C., Anderson, M., & Nolan.H. (2023). *How Americans view data privacy*. https://www.pewresearch.org/cloud/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/?form=MG0AV3

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, *21*. https://doi.org/10.3127/ajis.v21i0.1697

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McElroy, T., & Dowd, K. (2023). Susceptibility to anchoring effects: How openness-to-experience influences responses to anchoring cues. *Judgment and Decision Making*, 2(1), 48-53. https://doi.org/10.1017/S1930297500000279

Meertens, R. M., & Lion, R (2008). Measuring an individual's tendency to take risks: The risk propensity scale. *Journal of Applied Social Psychology, 38*(6), 1506-1520. https://doi.org/10.1111/j.1559-1816.2008.00357.x

Meinert, E., Alturkistani, A., Brindley, D., Knight, P., Wells, G., & de Pennington, N. (2018). Weighing benefits and risks in aspects of security, privacy and adoption of technology in a value-based healthcare system. *BMC Medical Informatics and Decision Making*, 18(1), 100. doi:10.1186/s12911-018-0700-0

Merians Penaloza, D. (2024). *Consumer Motivation and the Privacy Paradox* (Order No. 31146937). Available from ProQuest Dissertations & Theses Global. (3099750933). https://links.franklin.edu/login?url=https://www.proquest.com/dissertations-theses/consumer-motivation-privacy-paradox/docview/3099750933/se-2

Miglin, R., Bounoua, N., Goodling, S., Sheehan, A., Spielberg, J. M., & Sadeh, N (2019). Cortical thickness links impulsive personality traits and risky behavior, *Brain Science, 99*(12), 373. https://doi.org/10.3390/brainsci9120373

Mirsch, T., Lehrer, C., & Jung, R. (2017). *Digital nudging: Altering user behavior in digital environments*. https://aisel.aisnet.org/wi2017/track06/paper/4/

Moeller, F. G., Barratt, E. S., Dougherty, D. M., Schmitz, J. M., & Swann, A. C. (2001). Psychiatric aspects of impulsivity. *American Journal of Psychiatry, 158*(11), 1783-1793. https://doi.org/ 10.1176/appi.ajp.158.11.1783

Moreira, P. A. S., Inman, R. A., & Cloninger, C. R. (2023). Disentangling the personality pathways to well-being. *Scientific Reports, 13.* https://doi.org/10.1038/s41598-023-29642-5

Morgan, S. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Musafiri Mimo, E. (2022). *A Proactive Systematic Approach to Enhance and Preserve Users' Tech Applications Data Privacy Awareness and Control in Smart Cities* (Publication No.

2760074530) [Doctoral dissertation, Arizona State University]. ProQuest Dissertations & Theses Global.

Nasirpouri Shadbad, F. (2021). *Understanding Employee Non-malicious Intentional and Unintentional Information Security Misbehaviors* Publication No. 2585443123) [Doctoral dissertation, Oklahoma State University]. ProQuest Dissertations & Theses Global.

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

National Institute of Standards and Technology. (2025). *Glossary. Computer Security Resource Center*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Nedelec, J. L. (2018). Individual differences and co-occurring victimization online and offline: The role of impulsivity. *Personality and Individual Differences, 133,* 77-84. https://doi.org/10.1016/j.paid.2016.11.028

Németh, N., Péterfalvi, A., Czéh, B., Tényi, T., & Simon, M. (2020). Examining the relationship between executive functions and mentalizing abilities of patients with borderline personality disorder. *Frontiers in Psychology, 11.* https://doi.org/10.3389/fpsyg.2020.01583

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research, 8*(2), 157-196. https://doi.org//10.1080/1366987032000123856

Nifakos, S., Chandramouli, K., & Stathakarou, N. (2024). *Social Engineering: The Human Behavior Impact in Cyber Security Within Critical Information Infrastructures. In*

Security and Privacy in Smart Environments (pp. 173-184). Springer. https://doi.org/10.1007/978-3-031-66708-4_8

Office of the National Coordinator for Health Information Technology. (2023). *Health IT initiatives and interoperability advancements*. U.S. Department of Health and Human Services. https://www.congress.gov/crs_external_products/IF/PDF/IF12352/IF12352.3.pdf

Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science*, *17*(3), 57-74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Ostendorf, S., & Brand, M. (2022). Theoretical conceptualization of online privacy-related decision making—Introducing the tripartite self-disclosure decision model. *Frontiers in Psychology, 13.* https://www.frontiersin.org/articles/10.3389/fpsyg.2022.996512/full

Palinkas, L.A., et al. (2015) Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*, 533-544. https://doi.org/10.1007/s10488-013-0528-y

Park, W., Park, S., Choi, M., & Kim, K. (2021). A meta-analysis of impulsivity related to self-destructive behavior in Korean adolescents. J*ournal of Korean Academy of Community Health Nursing, 32*(3), 325-343. https://doi.org/10.12799/jkachn.2021.32.3.325

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, T. D., Barnett, M., & Melugin, P. R. (2015). Assessment of personality and absorption for mediated environments in a college sample. *Cyberpsychology, Behavior, and Social Networking, 18*(12), 752-756. https://doi.org/10.1089/cyber.2015.0336

Paspatis, I., Tsohou, A., & Kokolakis, S. (2023). How is privacy behavior formulated? A review of current research and synthesis of information privacy behavioral factors. *Multimodal Technologies and Interaction*, 7(8), 76. https://doi.org/10.3390/mti7080076

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Jerram, C. (2015). *Examining attitudes toward information security behavior using mixed methods. In S. Furnell & N. Clarke (Eds.), Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2015) (pp. 57–70). https://api.semanticscholar.org/CorpusID:2523982.

Pawlicka, A., Pawlicki, M., Kozik, R., & Choras, M. (2022). Human-driven and human-centered cybersecurity: Policy-making implications. *Transforming Government: People, Process and Policy, 16*(4), 478-487. https://doi.org/10.1108/TG-05-2022-0073

Peterka-Bonetta, J., Sindermann, C., Elhai, J. D., & Montag, C. (2019). Personality associations with smartphone and Cloud use disorder: A comparison study including links to impulsivity and social anxiety. *Frontiers in Psychology, 7.* https://doi.org/10.3389/fpubh.2019.00127

Petrosyan, A. (2025, March 7). *Most significant data breaches in the United States as of December 2024, by impact*. https://www.statista.com/statistics/1448545/us-biggest-data-breaches/

Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., Mendonça, F. L. L. d., de Oliveira Albuquerque, R., Sandoval Orozco, A. L., &

García Villalba, L. J. (2024). Understanding data breach from a global perspective: incident visualization and data protection law review. *Data, 9*(2), 27. https://doi.org/10.3390/data9020027

Prajapat, S., Gaur, A.S., Soni, P., Nagar, N., & Goswami, P. (2024). Cyber-attacks and review of recent data breach incidents their trends and measures. *Lecture Notes in Networks and Systems, 884*. https://doi.org/10.1007/978-3-031-74443-3_33

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*, 1299-1323. https://doi.org/10.1007/s11747-022-00845-y

Qualtrics. (2024). The survey data collection for this paper was generated using Qualtrics software, Version XM of Qualtrics. Copyright © [2024] Qualtrics.

Rachubinska, K., Cybulska, A., Szkup, M., & Grochans, E. (2021). Analysis of the relationship between personality traits and cloud addiction. *European Review of Medical and Pharmacological Sciences, 25,* 2591-2599. https://www.europeanreview.org/wp/wp-content/uploads/2591-2599.pdf

Rajesh, T., & Rangaiah, D. B. (2020). Facebook addiction and personality. *Heliyon*, *6*(1). https://doi.org/10.1016/j.heliyon.2020.e03184

Rammstedt, B., & John, O. P. (2007). Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. *Journal of Research in Personality, 41*(1), 203–212. https://doi.org/10.1016/j.jrp.2006.02.001

Rathore, A. (2019). A critical review of the effect of social networking sites on academic achievement among introverts and extroverts. *Seshadripuram Journal of Social Sciences, 1*(4), 68-73. https://mcom.sfgc.ac.in/downloads/onlin-journalagust-2019/A-critical-

review-on-effect-of-social-networking-sites-on-academic-acheivement-among-introverts-and-extroverts.pdf

Rizki, F. D., Chan, A., Barkah, C. S., & Tresna, P. W. (2022). The impact of Big Five Personality towards impulsive buying behavior. *International Journal of Entrepreneurship and Business Development,5,* 216-228. https://doi.org/10.29138/ijebd.v5i2.1733

Roberts, S. A. (2021). *Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors* (Publication No. 2506630550) [Doctoral dissertation, Northcentral University]. ProQuest Dissertations & Theses Global.

Rothmann, S., & Coetzer, E. P. (2003). The big five personality dimensions and job performance. *Journal of Industrial Psychology, 29.* https://doi.org/10.4102/sajip.v29i2.88

Rousseau, L. (2024). *The Impact of Data Harm on Data Privacy* (Publication No. 3152475289) [Doctoral dissertation, Marymount University]. ProQuest Dissertations & Theses Global.

Ruth, J. A. (2015). *An examination of the impact of the big five personality traits and work environment on the leadership behaviors of millennial generation employees* (Publication No. 1698459190) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses Global.

Ryan, E. (2024). *The Relationship Between Personality Traits and Emotional Intelligence in a Large Privately-Owned Manufacturing Organization* (Publication No. 3152435395) [Doctoral dissertation, The Chicago School]. ProQuest Dissertations & Theses Global.

Sadeghi, B., Richards, D., Formosa, P., McEwan, M., Bajwa, M. H. A., Hitchens, M., Ryan, M. (2023). Modelling the ethical priorities influencing decision-making in cybersecurity

contexts. *Organizational Cybersecurity Journal: Practice, Process and People, 3 (2),* 127–149. https://doi.org/10.1108/OCJ-09-2022-0015

Senyo, P. K., Liu, K., & Effah, J. (2019). Digital business ecosystem: Literature review and a framework for future research. *International Journal of Information Management, 47*, 52-64. https://doi.org/10.1016/j.ijinfomgt.2019.01.002

Serpico, L. (2020). *Personality, Digital Generation, and Social Media Integration as Predictors of Mindfulness* (Publication No. 2453679791) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses Global.

Nasirpouri Shadbad, F. (2021). *Understanding Employee Non-malicious Intentional and Unintentional Information Security Misbehaviors* (Publication No. 2585443123) [Doctoral dissertation, Oklahoma State University]. ProQuest Dissertations & Theses Global.

Shao, H., Li, X., & Wang, G. (2022). Are you tired? I am: Trying to understand privacy fatigue on social media users. *CHI EA '22, 378,* 1-7. https://doi.org/10.1145/3491101.3519778

Sharma, S., & Behl, R. (2022). Analyzing the impact of social media on students' academic performance: A comparative study of extraversion and introversion personality. *Psychological Studies, 67,* 549-559. https://doi.org/10.1007/s12646-022-00675-6

Shemeis, M., Asad, T., & Attia, S. (2021). The effect of Big Five factors of personality on compulsive buying: The mediating role of consumer negative emotions. *American Journal of Business Operations Research, 2*(1), 5-23. https://doi.org/10.5281/zenodo.4587359

Sichel, G. (2021). Public Awareness of Data Privacy and its Effects [Electronic thesis or dissertation, Ohio Dominican University]. OhioLINK Electronic Theses and

Dissertations Center. http://rave.ohiolink.edu/etdc/view?acc_num=oduhonors1620084176263829

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *Academy of Management Review, 17*(1). https://doi.org/10.5465/amr.1992.4279564

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196. https://doi.org/10.2307/249477

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016. https://doi.org/10.2307/41409970

Snipes, James B., III. (2024). *Evidence indicating the rise in insider threats in organizations and industries: A Quantitative Descriptive Study* (Publication No. 3066225580) [Doctoral dissertation, National University]. ProQuest Dissertations & Theses Global.

Stackpole, B (2024). *MIT report details new cybersecurity risks*. https://mitsloan.mit.edu/ideas-made-to-matter/mit-report-details-new-cybersecurity-risks

Starks, R. (2022). *Exploring the Current Challenges and Developing Reliable Measures to Guarantee the Best Security* (Publication No. 2744909527) [Doctoral dissertation, Northcentral University]. ProQuest Dissertations & Theses Global.

Stewart, J. C. (2020). *End-User Cloud Data Storage Experiences, Challenges, and Security Perceptions of the Emerging Technologies Security Tools among Small Businesses* (Publication No. 2416241575) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses Global.

Stewart, W. H., Jr., & Roth, P. L. (2001). Risk propensity differences between entrepreneurs and managers: A meta-analytic review. *Journal of Applied Psychology, 86*(1), 145-153. https://doi.org/10.1037/0021-9010.86.1.145

Stewart, K., & Segars, A. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*, 36-49. https://doi.org/10.1287/isre.13.1.36.97

Soomro, R. B., Memon, S. G., Dahri, Nisar Ahmed, Al-Rahmi, Waleed Mugahed, Aldriwish, K., Salameh, A., Al-Adwan, A. S., & Saleem, A. (2024). The adoption of digital technologies by small and medium-sized enterprises for sustainability and value creation in Pakistan: The application of a two-staged hybrid SEM-ANN approach. *Sustainability*, *16*(17), 7351. https://doi.org/10.3390/su16177351

Srabonee, J. F., Alharbi, O. M., Stuerzlinger, W., & Arif, A. S. (2025, April). *Exploring the impacts of HEXACO personality traits on text composition and transcription. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 577, 1-24. https://doi.org/10.1145/3706598.3714149

Stewart, W. H., Jr., & Roth, P. L. (2001). Risk propensity differences between entrepreneurs and managers: A meta-analytic review. *Journal of Applied Psychology*, *86*(1), 145-153. https://doi.org/10.1037/0021-9010.86.1.145

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications, 34*(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

Suntwal, S., Kocis, D., & Shepherd, M. M. (2025). Decrypting data breaches: An exploratory analysis of cyber fault lines across industry sectors and attack types. *The Geneva Papers*

on Risk and Insurance - Issues and Practice, *47*(3), 698–736. https://doi.org/10.2139/ssrn.5043413

Sürücü, L., & Maslakci, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal*, *8*(3), 2694–2726. https://doi.org/10.15295/bmij.v8i3.1540

Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews, 39*(1), 103-128. https://doi.org/10.1080/01441647.2018.1494640

U.S. Department of Health and Human Services. (2024). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. Office for Human Research Protections. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

Valasek, C. J. (2022). Disciplining the Akratic user: Constructing digital (un) wellness. *Mobile Media & Communication*, *10*(2), 235–250. https://doi.org/10.1177/20501579211038796

Verhaeghen, P., & Mirabito, G. (2021). When you are talking to yourself, was anybody listening? The relationship between inner speech, self-awareness, wellbeing, and multiple aspects of self-regulation. *International Journal of Personality Psychology, 7.* https://doi.org/10.21827/ijpp.7.37354

Verizon. (2024). *2024 Data breach investigations report*. https://www.verizon.com/business/resources/Tdd9/reports/2024-dbir-data-breach-investigations-report.pdf

Verizon. (2025, April 22). 2*025 Data breach investigations report*. https://www.verizon.com/business/resources/T1cf/reports/2025-dbir-data-breach-investigations-report.pdf

Villagran-Vizcarra, D. C., Luviano-Cruz, D., Pérez-Domínguez, L. A., Méndez-González, L. C., & Garcia-Luna, F. (2023). Applications analyses, challenges and development of augmented reality in education, industry, marketing, medicine, and entertainment. *Applied Sciences*, *13*(5), 2766. https://doi.org/10.3390/app13052766

von der Linden, D., te Nijenhuis, J., & Bakker, A. B. (2010). The general factor of personality: A meta-analysis of Big Five intercorrelations and a criterion-related validity study. *Journal of Research in Personality, 44*(3), 315-327. https://doi.org/10.1016/j.jrp.2010.03.003

Voss, E. (2023). *Insider Threat: A Case Study, Recognizing the Early Warnings Signs by Humans* (Publication No. 2844987035) [Doctoral dissertation, National University]. ProQuest Dissertations & Theses Global.

Wackler, A. (2021). *Dark triad and impulsivity.* https://shareok.org/handle/11244/332580

Wang, B., Han, Y., Wang, S., Tian, D., Cai, M., Liu, M., & Wang, L. (2022). A review of intelligent connected vehicle cooperative driving development. *Mathematics*, *10*(19), 3635. https://doi.org/10.3390/math1019

Watzlaf, V. J. M., DeAlmeida, D. R., Zhou, L., & Hartman, L. M. (2015). Protocol for systematic review in privacy and security in Telehealth: Best practices for healthcare professionals. *International Journal of Telerehabilitation*, *7*(15). https://doi.org/10.5195/IJT.2015.6186

Ward, S. (2019). *Diversity of personality as the facilitator of self-awareness.* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402199

Waranowicz, M. C. (2024). *Strategies for Successful Cybersecurity Implementation in New Jersey Public Schools* (Publication No. 3135042973) [Doctoral dissertation, WaldenUniversity]. ProQuest Dissertations & Theses Global.

Woods, N. (2022). *Users' Psychopathologies: Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior*. *In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security. Computational Methods in Applied Sciences, 56*. Springer, Cham. https://doi.org/10.1007/978-3-030-91293-2_5

Xu, H. (2020). Big five personality traits and ambiguity management in career decision-making. *The Career Development Quarterly*, *68*(2), 158–172. https://doi.org/10.1002/cdq.12220

Xu, X., Hong, W. C. H., Kolletar-Zhu, K., Zhang, Y., & Chi, C. (2023). Validation and application of the human aspects of information security questionnaire for undergraduates: effects of gender, discipline and grade level. *Behavior & Information Technology*, *43*(12), 2799–2820. https://doi.org/10.1080/0144929X.2023.2260876

Yadegari, Z., & Alinaghi, B. (2020). The effect of introversion and extroverts of individuals in the socialization of public space. *Technium Social Sciences Journal, 3,* 82-93. https://heinonline.org/HOL/LandingPage?handle=hein.journals/techssj3&div=10&id=&page=

Yahya, F. (2017). *A security framework to protect data in cloud storage* (Order No. 10958695). Available from ProQuest Dissertations & Theses Global. (2083754241). https://links.franklin.edu/login?url=https://www.proquest.com/dissertations-theses/security-framework-protect-data-cloud-storage/docview/2083754241/se-2

Yasin, A., Fatima, R., JiangBin, Z., Afzal, W., & Raza, S. (2024). Can serious gaming tactics bolster spear-phishing and phishing resilience? Securing the human hacking in

Information Security. *Information Software Technology*, *170*. https://doi.org/10.1016/j.infsof.2024.107426

Yamin, M. A. Y., & Alyoubi, B. A. (2020). Adoption of telemedicine applications among Saudi citizens during COVID-19 pandemic: An alternative health delivery system. *Journal of Infection and Public Health*, *13*, 1845–1855. https://doi.org/10.1016/j.jiph.2020.10.017

Zhang, D. C., Highhouse, S., & Nye, C. D. (2018). Development and validation of the General Risk Propensity Scale (GRiPS). *Journal of Behavioral Decision Making, 32*(2), 152-167. https://doi.org/10.1002/bdm.2102

Zhang, D. C., Barratt, C. L., & Smith, R. W. (2023). The bright, dark, and gray sides of risk takers at work: Criterion validity of risk propensity for contextual work performance. *Journal of Business and Psychology, 39.* https://doi.org//10.1007/s10869-023-09872-0

Zhang, W., He, L., Chen, Y., & Gao, X. (2024). The relationship between big five personality traits and fear of missing out: A meta-analysis. *Personality and Individual Differences*, *230*. https://doi.org/10.1016/j.paid.2024.112788

Zhang, J. (2025). *Understanding and managing integrated advanced persistent threats: Evaluation and analysis of large language models for phishing detection in small and midsize enterprises* (Order No. 32164182). Available from ProQuest Dissertations & Theses Global. (3232888722). https://links.franklin.edu/login?url=https://www.proquest.com/dissertations-theses/understanding-managing-integrated-advanced/docview/3232888722/se-2

Zhao, H., & Seibert, S. E. (2006). The Big Five personality dimensions and entrepreneurial status: A meta-analytical review. *Journal of Applied Psychology, 91*(2), 259-271. https://doi.org/10.1037/0021-9010.91.2.259

Appendix A: Institutional Review Board Approval Letter

FRANKLIN UNIVERSITY

Date: July 24, 2024
PI: Karuna Kothapalli
Department: Doctor of Business Admin, DBA
Re: Initial - IRB-2024-30
EXPLORING THE IMPACT OF MOTOR IMPULSIVITY ON CLOUD SECURITY BEHAVIOR WITHIN DIGITAL ENTERPRISES

The Franklin Institutional Review Board has rendered the decision below for *EXPLORING THE IMPACT OF MOTOR IMPULSIVITY ON CLOUD SECURITY BEHAVIOR WITHIN DIGITAL ENTERPRISES*.

Decision: Exempt
Category: Category 2.(i). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:
The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects;
Category 2.(ii). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:
Any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation; or

Findings: The PI will utilize an electronic survey (via Qualtrics) to explore the extent to which the Big Five personality characteristics moderate the relationship between impulsivity and the human aspects of cloud computing information security by privacy concerns in cloud security management.
Research Notes:

The IRB determination of exemption means:

- You must conduct the research as proposed in the Exempt application, including obtaining and documenting (signed) informed consent if stated in your application or if required by the IRB. You must use only the approved consent and assent forms (as applicable).
- Any modification of this research should be submitted to the IRB prior to implementation to determine if the study still meets federal exemption criteria.
- You are responsible for notifying the IRB Office with any problems or complaints about the research.
- **Students**, you will need to close your study prior to graduation.

Please also note the following:

- All investigators must keep their human subjects training current at www.citiprogram.org by renewing training every three (3) years.
- Detailed instructions for opening modification, closure, and incident submissions can be found on the Cayuse page of the IRB website.
- All approval letters and study documents are located within the Study Details in Cayuse.

You may contact the IRB Office at irb@franklin.edu with any questions.

Sincerely,

Franklin Institutional Review Board

Appendix B: Survey Questions

Quantitative Research Study – Qualtrics Survey Template

Q1. Informed Consent

Welcome to the research study!

We are interested in understanding impulsiveness and cloud security behavior. You will be presented with information relevant to Big Five personality traits, personal information privacy, and cyber security and asked to answer some questions about it. Please be assured that your responses will be kept completely confidential.

The study should take you around 10 minutes to complete, and you will receive ten dollars' worth of airline miles, gift cards, redeemable points, charitable donations, sweepstakes entrance, and vouchers for your participation. Your participation in this research is voluntary. You have the right to withdraw at any point during the study, for any reason, and without any prejudice. If you would like to contact the Principal Investigator in the study to discuss this research, please e-mail kothap01@email.franklin.edu.

By clicking the button below, you acknowledge that your participation in the study is voluntary, you are 18 years of age, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

Please note that this survey will be best displayed on a laptop or desktop computer. Some features may be less compatible for use on a mobile device.

- ○ I consent, begin the study
- ○ I do not consent, I do not wish to participate

Q2. How old are you?

- o 18-24 years old
- o 25-34 years old
- o 35-44 years old
- o 45-54 years old
- o 55-64 years old
- o 65+ years old

Q3. How do you describe yourself?

- o Male
- o Female
- o Non-binary/third gender
- o Prefer to self-describe

  [ ]

- o Prefer not to say

Q4. How long have you worked in cloud or cyber security industry?

- less than a year
- 1-5 years
- 5-10 years
- 10 years +

Q5. How long have you worked in cloud or cyber security industry?

- Business executive
- I.T. executive
- Business manager
- I.T. manager
- Cloud business and data security analyst
- Cloud business and data security architect
- Cloud business and data security engineer
- Other

Q6. I see myself as someone who…? Please indicate the extent to which you agree or disagree with each statement by selecting the number that corresponds to your response on the scale between 1 – 5 where 1 was “strongly disagree” and 5 “strongly agree” with each item?

	1. Strongly Disagree	2. Disagree a little	3. Neither agree nor disagree	4. Agree a little	5. Strongly agree
...is extraverted, enthusiastic	○	○	○	○	○
...is critical, quarrelsome	○	○	○	○	○
...dependable, self-disciplined	○	○	○	○	○
...is anxious, easily upset	○	○	○	○	○
...open to new experiences, complex	○	○	○	○	○
...is reserved, quite	○	○	○	○	○
...is sympathetic, warm	○	○	○	○	○
...is disorganized, careless	○	○	○	○	○
...is calm, emotionally stable	○	○	○	○	○
...is conventional, uncreative	○	○	○	○	○

Quantitative Research Study – Qualtrics Survey Template

Q7. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement. Please indicate the extent to which you agree or disagree with each statement by selecting the number that corresponds to your response on the scale between 1 – 5 where 1 was “strongly disagree” and 5 “strongly agree” with each item

	1. Strongly Disagree	2. Disagree a little	3. Neither agree nor disagree	4. Agree a little	5. Strongly agree
As an employee you should be concerned about data privacy and security	○	○	○	○	○
I think twice about providing my personal information to the external systems	○	○	○	○	○
I share less information with apps and services	○	○	○	○	○
I do not remove unused mobile apps and browser extensions	○	○	○	○	○
I do not ignore software or operating system updates	○	○	○	○	○

Q8. How often do you read privacy policies before agreeing to them?

- ○ Always
- ○ Sometimes
- ○ Never

Q9. How often do you read privacy policies before agreeing to them?

- ○ Use strong passwords
- ○ Enable two-factor authentication
- ○ Regularly updated software
- ○ Use a VPN
- ○ Tighten privacy settings on personal social media accounts
- ○ None of the above

Q10. How confident are you that companies protect your personal information adequately?

- ○ Very confident
- ○ Somewhat confident
- ○ Not confident

Q11. Do you think government regulations on data privacy are sufficient?

- Yes
- No
- Not sure

Q12. Have you ever been notified of a data breach involving your personal information?

- Yes
- No

Q13. How do you feel when targeted ads are based on your online activity?

- Comfortable
- Annoyed
- Concerned

Q14. How clear and understandable do you find the privacy policies of the cloud services you use?

- Very clear
- Somewhat clear
- Not clear

Q15. How clearly and understandable do you find malicious, negligent, and compromised insiders cause potential risk to cyber security?

- Very clear
- Somewhat clear
- Not clear

Q16. How do you rate yourself with impulsive data sharing? Please indicate the extent to which you agree or disagree with each statement by selecting the number that corresponds to your response on the scale between 1 – 4 where 1 was “Never” and 4 “Always” with each item

	1. Never	2. Rarely	3. Almost always	4. Always
I do things without thinking	○	○	○	○
I say things without thinking	○	○	○	○
I act "on impulse"	○	○	○	○
I act on the spur of the moment	○	○	○	○

Quantitative Research Study – Qualtrics Survey Template

Q17. How often do you behave like this in your workplace? Please indicate the extent to which you agree or disagree with each statement by selecting the number that corresponds to your response on the scale between 1 – 5 where 1 was "Always" and 5 "Never" with each item.

	1. Always	2. Very Frequently	3. Occassionally	4. Rarely	5. Never
I lock my computer if I leave it unattended	○	○	○	○	○
I share my personal password with others	○	○	○	○	○
I use passwords that are at least 10 characters long	○	○	○	○	○
I open the files that are attached to received e-mails, without any hesitation	○	○	○	○	○
If the e-mail seems legitimate, I click on the included links without hesitation	○	○	○	○	○
I put effort into educating myself in cybersecurity to understand which e-mails are secure	○	○	○	○	○
In my work computer I use software that originates from unofficial sources	○	○	○	○	○
I download files to my work computer only from legal sources	○	○	○	○	○
At my workplace, I visit web sites that are not connected to my work	○	○	○	○	○
I spend a part of my working time on social networking sites (doing activities not related to my work)	○	○	○	○	○
I click on links in social networking sites even if I am not sure that these links are safe enough to open	○	○	○	○	○
I consider the negative consequences (towards my job) before I post anything on social networking web sites	○	○	○	○	○
If I see a stranger at work, then I find out his/her purpose of visiting	○	○	○	○	○
I report unethical behavior of my colleagues (e.g. downloading illegal software, playing games during working hours, ignoring safety rules)	○	○	○	○	○
I share the information about all security incidents that happen to my work computer, with persons concerned	○	○	○	○	○
I leave my personal electronic devices (such as mobile phone or tablet computer) unattended	○	○	○	○	○
I use VPN when working remotely	○	○	○	○	○
I check work related email from public internet areas	○	○	○	○	○
I follow special procedures when disposing of sensitive documents to ensure that they cannot be read by third parties	○	○	○	○	○
I use USB devices without investigating whether the devices are infected by malware or not	○	○	○	○	○
I keep my work-related files encrypted (even on the external memory drives)	○	○	○	○	○

End of Survey

We thank you for your time spent taking this survey.

Your response has been recorded.

Appendix C: Data Analysis

Figure 11

Summary Statistics

Variable	Label	Mean	Std Dev	Minimum	Maximum	Median	N	N Miss	Std Error	Variance	Mode	Skewness	Kurtosis
MotorImpulsivity	MotorImpulsivity	2.0133333	0.6901674	1.0000000	3.7500000	2.0000000	150	0	0.0563519	0.4763311	2.0000000	0.6828928	0.1006933
OpennesstoExperience	OpennesstoExperience	3.4026667	0.4806241	2.6000000	4.6000000	3.3000000	150	0	0.0392428	0.2309996	3.1000000	0.6715258	-0.1525249
PersonalInformationPrivacy	PersonalInformationPrivacy	3.8613333	0.5298837	2.0000000	5.0000000	4.0000000	150	0	0.0432648	0.2807767	4.2000000	-0.6570984	0.5031619
IndividualBehavior	IndividualBehavior	2.8752381	0.5187639	1.4761905	3.8571429	2.9761905	150	0	0.0423569	0.2691180	2.9047619	-0.8467957	0.3617532
MI*OEP	MI*OEP	6.9400000	2.9912428	2.6000000	16.8750000	6.3000000	150	0	0.2442340	8.9475336	6.2000000	1.3789052	1.7772169
MI*PIP	MI*PIP	7.7326667	2.8384169	2.8000000	17.2500000	7.3500000	150	0	0.2317558	8.0566103	4.2000000	1.0568451	1.3084970

Note. The interaction variables are MI*OEP and MI*PIP.

Figure 12

SAS Output for Reliability Analysis

Cronbach Coefficient Alpha	
Variables	Alpha
Raw	0.879552
Standardized	0.886157

Cronbach Coefficient Alpha with Deleted Variable					
	Raw Variables		Standardized Variables		
Deleted Variable	Correlation with Total	Alpha	Correlation with Total	Alpha	Label
Q1	0.042170	0.881818	0.044458	0.887676	Q1
Q2	0.257137	0.879011	0.232742	0.885471	Q2
Q3	-.079951	0.882018	-.078098	0.889091	Q3
Q4	0.469107	0.875213	0.438062	0.883024	Q4
Q5	0.141701	0.879556	0.152632	0.886414	Q5
Q6	0.120035	0.880605	0.094492	0.887094	Q6
Q7	-.090748	0.882030	-.080939	0.889124	Q7
Q8	0.417902	0.876116	0.385833	0.883651	Q8
Q9	-.043291	0.881596	-.053474	0.888808	Q9
Q10	0.325337	0.877661	0.305532	0.884609	Q10
Q11	0.174300	0.879194	0.213625	0.885697	Q11
Q12	0.241188	0.878547	0.279886	0.884913	Q12
Q13	0.409731	0.876345	0.393175	0.883563	Q13
Q14	0.421751	0.876019	0.325795	0.884368	Q14
Q15	0.326271	0.877548	0.276268	0.884956	Q15
Q16	0.174300	0.879194	0.213625	0.885697	Q16
Q17	0.241188	0.878547	0.279886	0.884913	Q17
Q18	0.409731	0.876345	0.393175	0.883563	Q18
Q19	0.421751	0.876019	0.325795	0.884368	Q19
Q20	0.326271	0.877548	0.276268	0.884956	Q20
Q21	0.174300	0.879194	0.213625	0.885697	Q21
Q22	0.241188	0.878547	0.279886	0.884913	Q22
Q23	0.409731	0.876345	0.393175	0.883563	Q23
Q24	0.241188	0.878547	0.279886	0.884913	Q24
Q25	0.409731	0.876345	0.393175	0.883563	Q25
Q26	0.421751	0.876019	0.325795	0.884368	Q26
Q27	0.326271	0.877548	0.276268	0.884956	Q27
Q28	0.174300	0.879194	0.213625	0.885697	Q28
Q29	0.241188	0.878547	0.279886	0.884913	Q29
Q30	0.409731	0.876345	0.393175	0.883563	Q30
Q31	0.241188	0.878547	0.279886	0.884913	Q31
Q32	0.421751	0.876019	0.325795	0.884368	Q32
Q33	0.326271	0.877548	0.276268	0.884956	Q33
Q34	0.174300	0.879194	0.213625	0.885697	Q34
Q35	0.241188	0.878547	0.279886	0.884913	Q35
Q36	0.409731	0.876345	0.393175	0.883563	Q36
Q37	0.421751	0.876019	0.325795	0.884368	Q37
Q38	0.326271	0.877548	0.276268	0.884956	Q38
Q39	0.456560	0.876353	0.512048	0.882131	Q39
Q40	0.451508	0.876167	0.507074	0.882191	Q40
Q41	0.412781	0.876917	0.461843	0.882738	Q41
Q42	0.447688	0.876452	0.500164	0.882275	Q42
Q43	0.456560	0.876353	0.512048	0.882131	Q43
Q44	0.451508	0.876167	0.507074	0.882191	Q44
Q45	0.409731	0.876345	0.393175	0.883563	Q45
Q46	0.421751	0.876019	0.325795	0.884368	Q46
Q47	0.326271	0.877548	0.276268	0.884956	Q47
Q48	0.456560	0.876353	0.512048	0.882131	Q48
Q49	0.451508	0.876167	0.507074	0.882191	Q49
Q50	0.412781	0.876917	0.461843	0.882738	Q50
Q51	0.447688	0.876452	0.500164	0.882275	Q51
Q52	0.456560	0.876353	0.512048	0.882131	Q52
Q53	0.451508	0.876167	0.507074	0.882191	Q53
Q54	0.412781	0.876917	0.461843	0.882738	Q54
Q55	0.447688	0.876452	0.500164	0.882275	Q55
Q56	0.451508	0.876167	0.507074	0.882191	Q56
Q57	0.412781	0.876917	0.461843	0.882738	Q57
Q58	0.447688	0.876452	0.500164	0.882275	Q58
Q59	0.456560	0.876353	0.512048	0.882131	Q59
Q60	0.451508	0.876167	0.507074	0.882191	Q60
Q61	-.112945	0.883443	-.125097	0.889630	Q61
Q62	-.324856	0.886410	-.318946	0.891827	Q62
Q63	-.078774	0.882670	-.093660	0.889270	Q63

Note. Cronbach's $\alpha \geq 0.70$ was acceptable for each question.

Figure 13

SAS Output Principal Component Analysis

The FACTOR Procedure
Initial Factor Method: Principal Components

Prior Communality Estimates: ONE

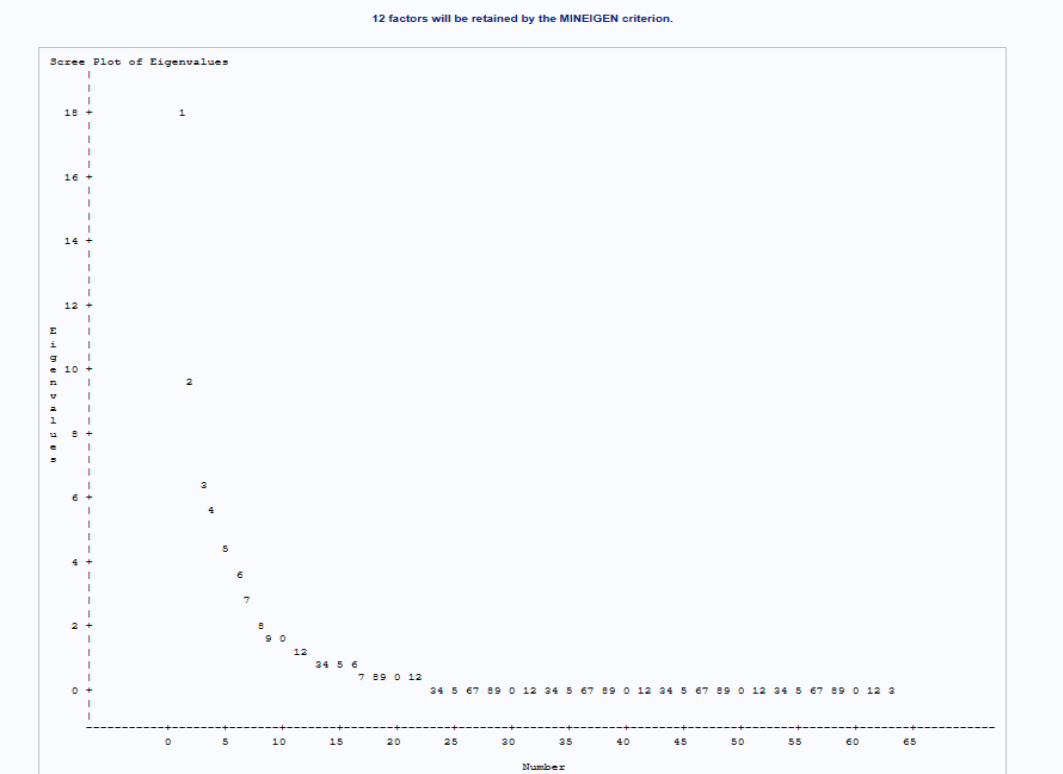
Eigenvalues of the Correlation Matrix: Total = 63 Average = 1

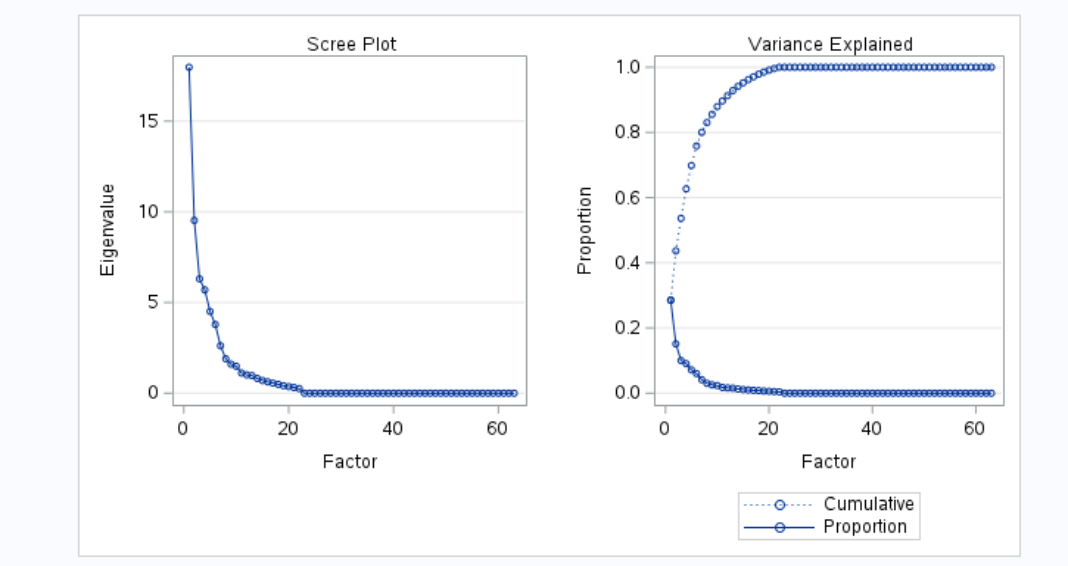
	Eigenvalue	Difference	Proportion	Cumulative
1	17.9723468	8.4451012	0.2853	0.2853
2	9.5272457	3.2242398	0.1512	0.4365
3	6.3030058	0.6084241	0.1000	0.5365
4	5.6945817	1.1887525	0.0904	0.6269
5	4.5058292	0.7182610	0.0715	0.6985
6	3.7875682	1.1721900	0.0601	0.7586
7	2.6153783	0.7191862	0.0415	0.8001
8	1.8961921	0.2944373	0.0301	0.8302
9	1.6017548	0.1176754	0.0254	0.8556
10	1.4840794	0.3725830	0.0236	0.8792
11	1.1114964	0.0997026	0.0176	0.8968
12	1.0117938	0.0443120	0.0161	0.9129
13	0.9674819	0.1545242	0.0154	0.9282
14	0.8129577	0.1157721	0.0129	0.9411
15	0.6971856	0.0723760	0.0111	0.9522
16	0.6248096	0.0740015	0.0099	0.9621
17	0.5508081	0.0601859	0.0087	0.9709
18	0.4906222	0.0774718	0.0078	0.9787
19	0.4131504	0.0497986	0.0066	0.9852
20	0.3633518	0.0504365	0.0058	0.9910
21	0.3129153	0.0574700	0.0050	0.9959
22	0.2554453	0.2554453	0.0041	1.0000
23	0.0000000	0.0000000	0.0000	1.0000
24	0.0000000	0.0000000	0.0000	1.0000
25	0.0000000	0.0000000	0.0000	1.0000
26	0.0000000	0.0000000	0.0000	1.0000
27	0.0000000	0.0000000	0.0000	1.0000
28	0.0000000	0.0000000	0.0000	1.0000
29	0.0000000	0.0000000	0.0000	1.0000
30	0.0000000	0.0000000	0.0000	1.0000

Note. Components with Eigenvalues ≥ 1 were meaningful and retained.

Figure 14

SAS PCA Output Scree Plots





Note. Components with Eigenvalues ≥ 1 were meaningful and retained and a flat line observed after the elbow point.

Figure 15

Individual Behavior (outcome variable) Box-Cox Transformation

Variable: IndividualBehavior_BoxCox

Moments			
N	420	Sum Weights	420
Mean	7.06500928	Sum Observations	2967.3039
Std Deviation	0.79152572	Variance	0.62651297
Skewness	-0.1075278	Kurtosis	-0.2314545
Uncorrected SS	21226.5385	Corrected SS	262.508935
Coeff Variation	11.2034633	Std Error Mean	0.0386225

Basic Statistical Measures			
Location		Variability	
Mean	7.065009	Std Deviation	0.79153
Median	7.020713	Variance	0.62651
Mode	6.926496	Range	4.41027
		Interquartile Range	1.11174

Note: The mode displayed is the smallest of 2 modes with a count of 16.

Tests for Location: Mu0=0				
Test	Statistic		p Value	
Student's t	t	182.9247	Pr > |t|	<.0001
Sign	M	210	Pr >= |M|	<.0001
Signed Rank	S	44205	Pr >= |S|	<.0001

Tests for Normality				
Test	Statistic		p Value	
Shapiro-Wilk	W	0.996598	Pr < W	0.5209
Kolmogorov-Smirnov	D	0.03821	Pr > D	0.1395
Cramer-von Mises	W-Sq	0.058171	Pr > W-Sq	>0.2500
Anderson-Darling	A-Sq	0.355428	Pr > A-Sq	>0.2500

Note. Statistical normality assumption was met as Shapiro-Wilk $p > .001$.

Figure 16

Motor Impulsivity (dependent variable) Box-Cox Transformation

Variable: MotorImpulsivity_BoxCox

Moments			
N	420	Sum Weights	420
Mean	22.9716064	Sum Observations	9648.07469
Std Deviation	4.07670734	Variance	16.6195428
Skewness	0.06941896	Kurtosis	-0.2826591
Uncorrected SS	228595.363	Corrected SS	6963.58841
Coeff Variation	17.7467229	Std Error Mean	0.19892295

Basic Statistical Measures			
Location		Variability	
Mean	22.97161	Std Deviation	4.07671
Median	22.60528	Variance	16.61954
Mode	22.12187	Range	22.59227
		Interquartile Range	5.76068

Note: The mode displayed is the smallest of 2 modes with a count of 16.

Tests for Location: Mu0=0				
Test	Statistic		p Value	
Student's t	t	115.4799	Pr > |t|	<.0001
Sign	M	210	Pr >= |M|	<.0001
Signed Rank	S	44205	Pr >= |S|	<.0001

Tests for Normality				
Test	Statistic		p Value	
Shapiro-Wilk	W	0.996797	Pr < W	0.5778
Kolmogorov-Smirnov	D	0.042943	Pr > D	0.0589
Cramer-von Mises	W-Sq	0.064859	Pr > W-Sq	>0.2500
Anderson-Darling	A-Sq	0.385101	Pr > A-Sq	>0.2500

Note. Statistical normality assumption was met as Shapiro-Wilk $p > .001$.

Figure 17

Openness to Experience (moderator variable) Box-Cox Transformation

Variable: OpennessToExp_BoxCox

Moments			
N	420	Sum Weights	420
Mean	50.5393774	Sum Observations	21226.5385
Std Deviation	11.1479261	Variance	124.276256
Skewness	0.18386945	Kurtosis	-0.2632402
Uncorrected SS	1124847.79	Corrected SS	52071.7514
Coeff Variation	22.0579015	Std Error Mean	0.54396309

Basic Statistical Measures			
Location		Variability	
Mean	50.53938	Std Deviation	11.14793
Median	49.29041	Variance	124.27626
Mode	47.97635	Range	61.76084
		Interquartile Range	15.76873

Note: The mode displayed is the smallest of 2 modes with a count of 16.

Tests for Location: Mu0=0				
Test	Statistic		p Value	
Student's t	t	92.90957	Pr > |t|	<.0001
Sign	M	210	Pr >= |M|	<.0001
Signed Rank	S	44205	Pr >= |S|	<.0001

Tests for Normality				
Test	Statistic		p Value	
Shapiro-Wilk	W	0.994857	Pr < W	0.1752
Kolmogorov-Smirnov	D	0.051745	Pr > D	<0.0100
Cramer-von Mises	W-Sq	0.099087	Pr > W-Sq	0.1184
Anderson-Darling	A-Sq	0.596839	Pr > A-Sq	0.1236

Note. Statistical normality assumption was met as Shapiro-Wilk $p > .001$.

Figure 18

Personal Information Privacy (mediator variable) Box-Cox Transformation

Variable: PersonalInfPrivacy_BoxCox

Moments			
N	420	Sum Weights	420
Mean	3.22703917	Sum Observations	1355.35645
Std Deviation	0.21861245	Variance	0.0477914
Skewness	-0.2298632	Kurtosis	-0.1382939
Uncorrected SS	4393.81296	Corrected SS	20.0245976
Coeff Variation	6.77439709	Std Error Mean	0.0106672

Basic Statistical Measures			
Location		Variability	
Mean	3.227039	Std Deviation	0.21861
Median	3.219799	Variance	0.04779
Mode	3.193803	Range	1.22660
		Interquartile Range	0.30486

Note: The mode displayed is the smallest of 2 modes with a count of 16.

Tests for Location: Mu0=0				
Test	Statistic		p Value	
Student's t	t	302.5199	Pr > |t|	<.0001
Sign	M	210	Pr >= |M|	<.0001
Signed Rank	S	44205	Pr >= |S|	<.0001

Tests for Normality				
Test	Statistic		p Value	
Shapiro-Wilk	W	0.994266	Pr < W	0.1165
Kolmogorov-Smirnov	D	0.044245	Pr > D	0.0445
Cramer-von Mises	W-Sq	0.084701	Pr > W-Sq	0.1865
Anderson-Darling	A-Sq	0.534132	Pr > A-Sq	0.1785

Note. Statistical normality assumption was met as Shapiro-Wilk $p > .001$.

Figure 19

SPSS Output of Linear Regression to test Multicollinearity

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.327[a]	.107	.088	.49532598198	2.167

a. Predictors: (Constant), MIPIP, MIOEP, MI

b. Dependent Variable: IB

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.277	3	1.426	5.811	<.001[b]
	Residual	35.821	146	.245		
	Total	40.098	149			

a. Dependent Variable: IB

b. Predictors: (Constant), MIPIP, MIOEP, MI

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	3.334	.131		25.500	<.001		
	MI	-.114	.141	-.152	-.809	.420	.174	5.753
	MIOEP	-.009	.015	-.052	-.636	.526	.920	1.087
	MIPIP	-.030	.034	-.164	-.872	.385	.173	5.769

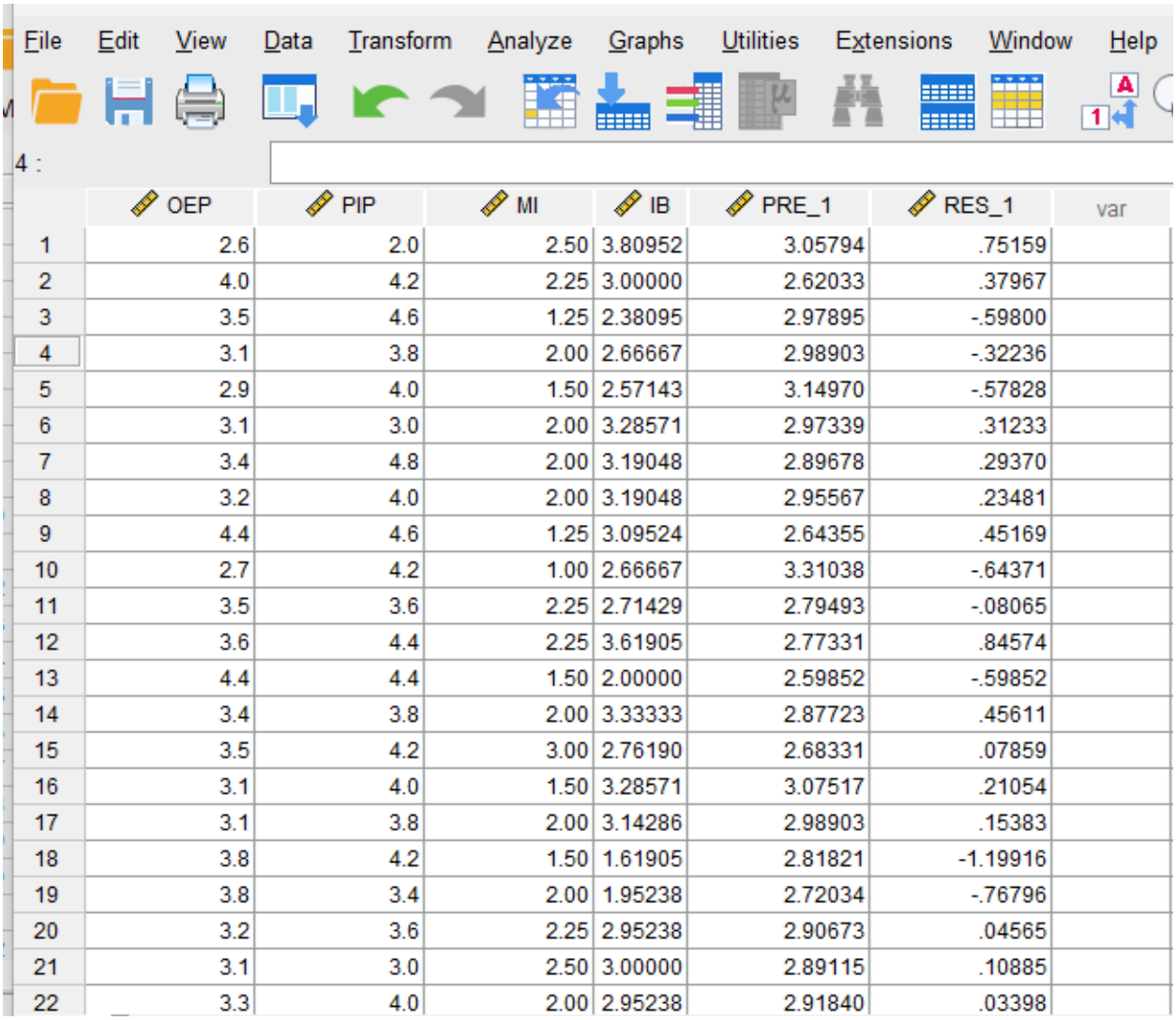
a. Dependent Variable: IB

Note. VIF values of MI, MI*OEP, MI*PIP VIF values were less than 10 and Tolerance is greater than 0.1.

.

Figure 20

SPSS Data View with Predictor and Residual Values

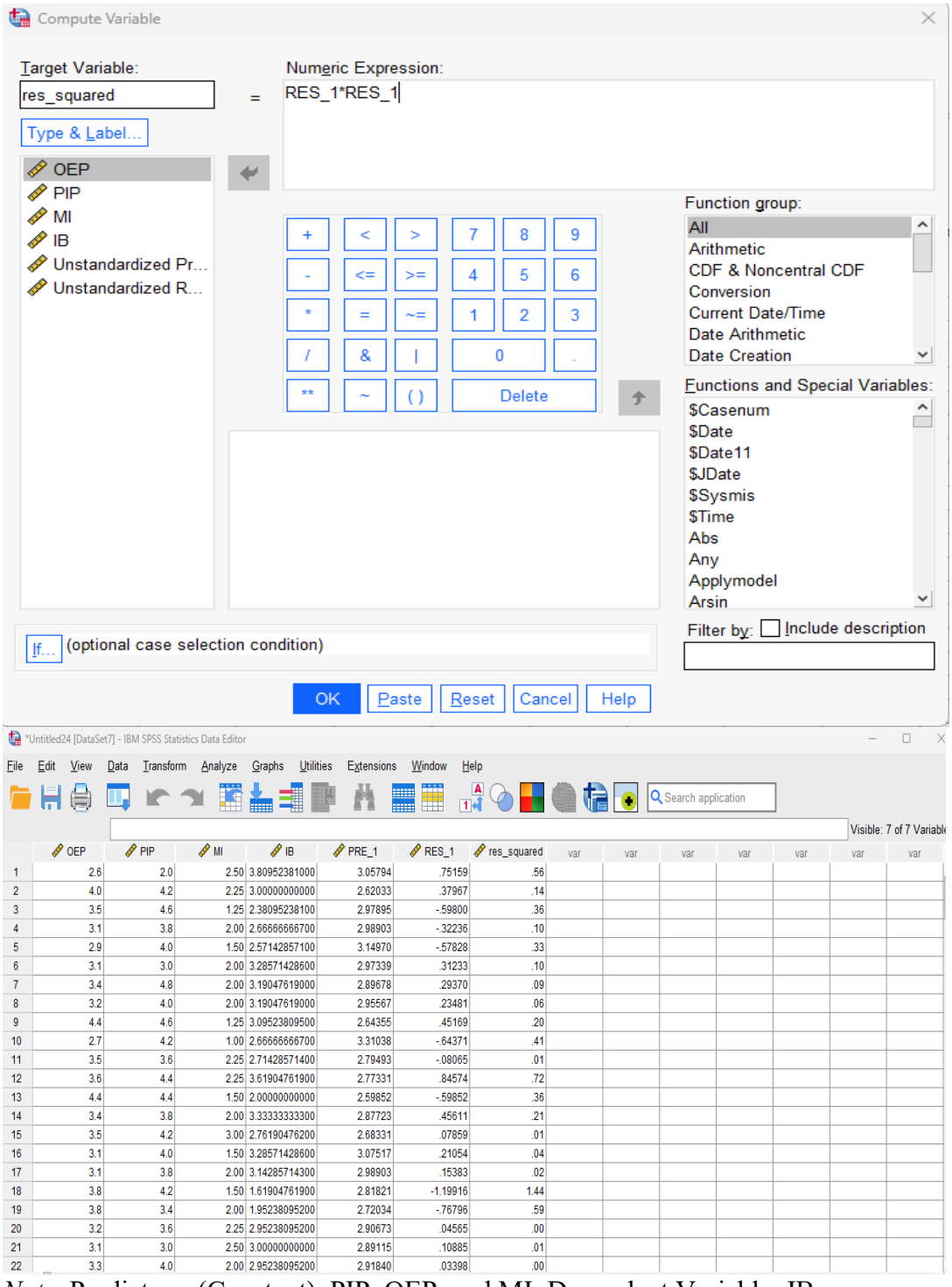


	OEP	PIP	MI	IB	PRE_1	RES_1	var
1	2.6	2.0	2.50	3.80952	3.05794	.75159	
2	4.0	4.2	2.25	3.00000	2.62033	.37967	
3	3.5	4.6	1.25	2.38095	2.97895	-.59800	
4	3.1	3.8	2.00	2.66667	2.98903	-.32236	
5	2.9	4.0	1.50	2.57143	3.14970	-.57828	
6	3.1	3.0	2.00	3.28571	2.97339	.31233	
7	3.4	4.8	2.00	3.19048	2.89678	.29370	
8	3.2	4.0	2.00	3.19048	2.95567	.23481	
9	4.4	4.6	1.25	3.09524	2.64355	.45169	
10	2.7	4.2	1.00	2.66667	3.31038	-.64371	
11	3.5	3.6	2.25	2.71429	2.79493	-.08065	
12	3.6	4.4	2.25	3.61905	2.77331	.84574	
13	4.4	4.4	1.50	2.00000	2.59852	-.59852	
14	3.4	3.8	2.00	3.33333	2.87723	.45611	
15	3.5	4.2	3.00	2.76190	2.68331	.07859	
16	3.1	4.0	1.50	3.28571	3.07517	.21054	
17	3.1	3.8	2.00	3.14286	2.98903	.15383	
18	3.8	4.2	1.50	1.61905	2.81821	-1.19916	
19	3.8	3.4	2.00	1.95238	2.72034	-.76796	
20	3.2	3.6	2.25	2.95238	2.90673	.04565	
21	3.1	3.0	2.50	3.00000	2.89115	.10885	
22	3.3	4.0	2.00	2.95238	2.91840	.03398	

Note. Predictors: (Constant), PIP, OEP, and MI; Dependent Variable: IB.

Figure 21

SPSS Computation of Squared Residuals



	OEP	PIP	MI	IB	PRE_1	RES_1	res_squared	var	var	var	var	var	var	var
1	2.6	2.0	2.50	3.80952381000	3.05794	.75159	.56							
2	4.0	4.2	2.25	3.00000000000	2.62033	.37967	.14							
3	3.5	4.6	1.25	2.38095238100	2.97895	-.59800	.36							
4	3.1	3.8	2.00	2.66666666700	2.98903	-.32236	.10							
5	2.9	4.0	1.50	2.57142857100	3.14970	-.57828	.33							
6	3.1	3.0	2.00	3.28571428600	2.97339	.31233	.10							
7	3.4	4.8	2.00	3.19047619000	2.89678	.29370	.09							
8	3.2	4.0	2.00	3.19047619000	2.95567	.23481	.06							
9	4.4	4.6	1.25	3.09523809500	2.64355	.45169	.20							
10	2.7	4.2	1.00	2.66666666700	3.31038	-.64371	.41							
11	3.5	3.6	2.25	2.71428571400	2.79493	-.08065	.01							
12	3.6	4.4	2.25	3.61904761900	2.77331	.84574	.72							
13	4.4	4.4	1.50	2.00000000000	2.59852	-.59852	.36							
14	3.4	3.8	2.00	3.33333333300	2.87723	.45611	.21							
15	3.5	4.2	3.00	2.76190476200	2.68331	.07859	.01							
16	3.1	4.0	1.50	3.28571428600	3.07517	.21054	.04							
17	3.1	3.8	2.00	3.14285714300	2.98903	.15383	.02							
18	3.8	4.2	1.50	1.61904761900	2.81821	-1.19916	1.44							
19	3.8	3.4	2.00	1.95238095200	2.72034	-.76796	.59							
20	3.2	3.6	2.25	2.95238095200	2.90673	.04565	.00							
21	3.1	3.0	2.50	3.00000000000	2.89115	.10885	.01							
22	3.3	4.0	2.00	2.95238095200	2.91840	.03398	.00							

Note. Predictors: (Constant), PIP, OEP, and MI; Dependent Variable: IB.

Figure 22

SPSS Output ANOVA Homoscedasticity

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.182[a]	.033	.013	.35220	1.846

a. Predictors: (Constant), MIPIP, MIOEP, MI

b. Dependent Variable: res_squared

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.620	3	.207	1.667	.177[b]
	Residual	18.111	146	.124		
	Total	18.731	149			

a. Dependent Variable: res_squared

b. Predictors: (Constant), MIPIP, MIOEP, MI

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.147	.093		1.579	.116		
	MI	.106	.100	.206	1.057	.292	.174	5.753
	MIOEP	.016	.011	.126	1.483	.140	.920	1.087
	MIPIP	-.015	.024	-.122	-.625	.533	.173	5.769

a. Dependent Variable: res_squared

Note. ANOVA p-value >0.05 indicated homoscedasticity normality assumption was met.

Figure 23

Mediation Analysis – Independent and Mediator predicting the outcome

```
Run MATRIX procedure:

***************** PROCESS Procedure for SPSS Version 4.2 *****************

          Written by Andrew F. Hayes, Ph.D.       www.afhayes.com
    Documentation available in Hayes (2022). www.guilford.com/p/hayes3

**************************************************************************
Model  : 4
    Y  : IB
    X  : MI
    M  : PIP

Sample
Size:  150

**************************************************************************
OUTCOME VARIABLE:
 PIP

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .2279      .0519      .3641     8.1073     1.0000   148.0000      .0050

Model
              coeff         se          t          p       LLCI       ULCI
constant     2.8103      .1413    19.8949      .0000     2.5311     3.0894
MI           -.2134      .0749    -2.8473      .0050     -.3615     -.0653

Standardized coefficients
        coeff
MI     -.2279

**************************************************************************
OUTCOME VARIABLE:
 IB

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .2781      .0773     1.4435     6.1601     2.0000   147.0000      .0027

Model
              coeff         se          t          p       LLCI       ULCI
constant     5.8281      .5392    10.8098      .0000     4.7626     6.8936
MI           -.3063      .1532    -1.9988      .0475     -.6092     -.0035
PIP          -.5344      .1637    -3.2649      .0014     -.8578     -.2109

Standardized coefficients
         coeff
MI      -.1626
PIP     -.2657
```

Note. Both models are significant (p<.05) and MI = motor impulsivity; PIP = personal information privacy; IB = individual behavior.

Figure 24

Boot Strap Procedure

```
************** TOTAL, DIRECT, AND INDIRECT EFFECTS OF X ON Y **************

Total effect of X on Y
     Effect         se          t          p       LLCI       ULCI       c_cs
     -.1923      .1540    -1.2486      .2138     -.4966      .1120     -.1021

Direct effect of X on Y
     Effect         se          t          p       LLCI       ULCI      c'_cs
     -.3063      .1532    -1.9988      .0475     -.6092     -.0035     -.1626

Indirect effect(s) of X on Y:
        Effect     BootSE   BootLLCI   BootULCI
PIP      .1140      .0532      .0289      .2332

Completely standardized indirect effect(s) of X on Y:
        Effect     BootSE   BootLLCI   BootULCI
PIP      .0605      .0273      .0154      .1205

************************ ANALYSIS NOTES AND ERRORS ************************

Level of confidence for all confidence intervals in output:
  95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:
  5000

------ END MATRIX -----
```

Note. Indirect effect = MI ⟶ IB (controlling PIP)

Figure 25

Moderation Analysis – Predictor and Moderator Model Significance

```
**************************************************************************
Model  : 1
    Y  : IB
    X  : MI
    W  : OEP

Sample
Size:  150

**************************************************************************
OUTCOME VARIABLE:
 IB

Model Summary
          R       R-sq        MSE          F        df1        df2          p
      .7459      .5564     6.5195    61.0501     3.0000   146.0000      .0000

Model
             coeff         se          t          p       LLCI       ULCI
constant    6.0147      .2085    28.8423      .0000     5.6025     6.4268
MI           .2630      .0205    12.8492      .0000      .2226      .3035
OEP         -.0008      .0003    -2.9849      .0033     -.0014     -.0003
Int_1        .0001      .0000     2.4582      .0151      .0000      .0001

Product terms key:
 Int_1    :        MI       x        OEP

Test(s) of highest order unconditional interaction(s):
       R2-chng           F        df1        df2          p
X*W      .0184     6.0427     1.0000   146.0000      .0151
----------
    Focal predict: MI       (X)
          Mod var: OEP      (W)

Conditional effects of the focal predictor at values of the moderator(s):

        OEP     Effect         se          t          p       LLCI       ULCI
  -887.7267      .2177      .0203    10.7358      .0000      .1776      .2578
      .0000      .2630      .0205    12.8492      .0000      .2226      .3035
   887.7267      .3083      .0332     9.2738      .0000      .2426      .3740

************************ ANALYSIS NOTES AND ERRORS ************************

Level of confidence for all confidence intervals in output:
  95.0000

W values in conditional tables are the mean and +/- SD from the mean.

NOTE: The following variables were mean centered prior to analysis:
          OEP      MI
```

Note: Adjusted ΔR^2 variance = 2% after the interaction with significance ($p<.05$); Int_1 = MI*OEP.

Appendix D: Program Outcome Measures

This dissertation met the Doctorate of Business Administration (DBA) Program Outcomes as outlined by Franklin University by fulfilling all essential components required for a business-focused doctoral dissertation.

BSADD1: Perform scholarly research and composition essential for the production of a business-focused doctoral dissertation

BSADD2: Apply and integrate current research and scholarly-based literature contributing to a significant field of business administration

BSADD5: Interpret and explain scholarly-based leadership, cultural, systems-thinking, and organizational change theoretical underpinnings essential for business effectiveness

BSADD6: Design and defend scholarly research that contributes to the professional body of knowledge for effective business

The doctoral candidate demonstrated the ability to perform scholarly research and composition, through the rigorous investigation the research situated itself within the broader academic discourse, contributing valuable insights and extending the existing knowledge base. Integrating diverse sources and perspectives underscores the candidate's ability to critically engage with and synthesize scholarly literature to support their arguments and findings.