CERIAS Tech Report 2026-01
Personality Influences on Cyber Intrusion Behavior: A Mixed-Methods Analysis
by Rachel Anne Sitarz
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

PERSONALITY INFLUENCES ON CYBER INTRUSION BEHAVIOR: A MIXED-METHODS ANALYSIS

by

Rachel Sitarz

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Computer and Information Technology

West Lafayette, Indiana

May 2026

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Marcus Rogers, Chair
Purdue Polytechnic Institute

Dr. Tatiana Ringenberg
Purdue Polytechnic Institute

Dr. John Springer
Purdue Polytechnic Institute

Dr. Dustin Hutchison
Pondurance

Approved by:
Dr. Stephen J. Elliott

In 2011, my dad, John Sitarz, passed away from esophageal cancer. Before he passed, he said to me, "Promise you will be the first Sitarz to become a doctor." While this degree has taken quite a long time to complete, finally, I have always been dedicated to finishing it for him.

Dad – thank you for believing in me. Thank you for being the angel on my shoulder, guiding me to complete this. Even when I thought I could not do it, I stayed the course for you. I hope you are in Heaven and are proud of this accomplishment. I wish you could be here to see it.

Mom – thank you for supporting me through this journey. You have helped so much by watching Roman when I needed to be heads-down working. I cannot express how much that has meant.

Caleb – thank you for being there for me through this. This has been a goal long before we got married, and I am so grateful for the support. It has not been easy, but you have been my rock and have been there for me along the way. I love you and am so grateful for a husband as great as you.

Roman – my baby boy. I love you so much. You are 4 right now, and seeing me work through this, I hope, will bring so much motivation to your life. I know you are going to do even bigger and better things than I can ever imagine. I know I had to give up some play time with you so I could work on my "puter" throughout this journey. I hope you know that this has all been for you. You are the best thing that has ever happened to mommy and daddy. This accomplishment is for you. I love you more than pizza, candy, and all the things.

I also cannot forget to thank Dr. Rogers and my committee for believing in me and allowing me to go through this process on my time. It has taken far longer than I expected, but you allowed me to finish this up, and I am so grateful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Research on cyber intrusion mainly focuses on technical systems, operational security, and specific vulnerabilities, often overlooking individual differences in attackers' decision-making. This mixed-methods study explored how Dark Triad and Big Five personality traits influence cyber intrusion behaviors in a simulated tabletop exercise. The aim was to understand how personality impacts both the choice and execution of intrusion strategies.

Of the 257 participants who completed the personality assessments, 196 provided complete responses to the intrusion scenario aligned with the MITRE ATT&CK Framework. The quantitative analyses included correlation tests, binary logistic regression, moderation analyses, and Random Forest validation to evaluate predictive consistency. Open-ended responses were analyzed qualitatively and thematically coded for specific behaviors such as reconnaissance, deception, persistence, creativity, and aggression.

Results indicated that Dark Triad traits are connected to risk-intrusion behaviors. Psychopathy predicted persistence, boldness, and high-risk tactics; Machiavellianism was linked to deception and manipulation. Narcissism had a limited but significant effect. The Big Five traits mainly influenced cognitive and procedural styles: Conscientiousness for structured behaviors, Openness for creativity, and Extraversion for assertiveness. Age and cybersecurity involvement modify these relationships, highlighting developmental and experiential factors.

Qualitative findings reinforced the quantitative results, showing intrusion decision-making as dynamic and multi-phased rather than linear. The findings support a person-situation interaction framework, highlighting that cyber intrusion decision-making involves personality traits, context, and technical expertise. Although exploratory, this study underscores the importance of human factors in cybersecurity research and practice.

INTRODUCTION

Cyber-attacks and data breaches have increased significantly and become more sophisticated over the past decades, largely due to the growing reliance on technology by organizations and individuals (Maxmillian & Sinha, 2022). This dependence has resulted in an ever-changing threat landscape, with cyber-attacks becoming more advanced, innovative, and complex (Maxmillian & Sinha, 2022; Verizon, 2024). Cybersecurity experts and organizations frequently publish technical reports on cyber threats and incidents, providing essential threat intelligence that helps defenders strengthen their security measures and adopt proactive defense strategies (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020). However, a crucial aspect often missing in these technical documents is the attacker's personality (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020). Gaining insights into personality and its impact on decision-making during cyber-attacks can improve defensive efforts and better safeguard critical data and infrastructure (Al-Shaer et al., 2020; Belfadel et al., 2022; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020).

The growing interconnectedness of technology has led to numerous opportunities for cyber-attacks and data breaches. The growth in incidents is driven by a significant increase in identified vulnerabilities, along with the constantly changing tactics and techniques used by threat actors (Budimir et al., 2021; Gaia et al., 2020; Kennison & Chan-Tin, 2021; Ma, 2021; Olufunsho et al., 2022; Sailio et al., 2020). Rapid technological advancements, such as Artificial Intelligence, have also made system structures more complex, creating more opportunities for cyber threats (Budimir et al., 2021; Cai et al., 2023; Liang et al., 2022; Ma, 2021; Sailio et al., 2020). These technological advances have spurred the growth of cybercriminal organizations and increased the chances of cyber-attacks (Budimir et al., 2021; Ma, 2021; Olufunsho et al., 2022).

The ease of access and use of these technologies, together with rising vulnerabilities in systems, have expanded the scope of cyber threats and the number of people capable of launching attacks (Kennison & Chan-Tin, 2021; Maslej et al., 2024; Sailio et al., 2020; Wang et al., 2023). As the attack surface widens and the reliance on technology deepens worldwide, defending against cyber-attacks becomes more complex and demanding, highlighting the need for comprehensive, adaptive, and behaviorally-informed defensive strategies (Cai et al., 2023; Liang et al., 2022; Olufunsho et al., 2022; Romanosky & Boudreaux, 2021; Sailio et al., 2020).

Understanding the personality types of threat actors (also called hackers) and how their personalities influence intrusion decision-making can help security professionals create more effective proactive defenses. However, access to these individuals is difficult (Basak, 2018; Curtis et al., 2021; Jones et al., 2021; Jones, 2022). They often operate in hidden parts of the internet, usually requiring personal invitations and vetting by other hackers (Benjamin et al., 2019). These platforms are where they share information, exchange technical resources, and form partnerships (Benjamin et al., 2019; Ding et al., 2021; Pastrana et al., 2018). Because hackers operate in highly controlled environments, researching and reaching this group is challenging (Benjamin et al., 2019). Nonetheless, understanding their personalities and how these traits shape their Tactics, Techniques, and Procedures (TTPs) can significantly aid cybersecurity strategies, leading to better prevention and defense against future cyber-attacks (Jones, 2022; Maxmillian & Sinha, 2022; Verizon, 2024).

It is widely recognized that personality traits influence individual decision-making (Basak et al., 2018; Curtis et al., 2021). Personality is flexible and varies significantly among individuals (Basak et al., 2018; Curtis et al., 2021). These differences result in unique behavioral outcomes shaped by each person's specific personality characteristics (Basak et al., 2018; Curtis

et al., 2021). However, limited information is available regarding hacker personalities and their correlation with cyber threat behaviors (Gaia et al., 2020; Gaia et al., 2022; Jones et al., 2021). Previous research on hacker personality types has examined factors such as perceptions of fear or workplace misconduct; however, this research does not clarify how personality influences the choice of TTPs and attack techniques (Fagade et al., 2017; Gaia et al., 2020; Gaia et al., 2022; Jones et al., 2021; Maasberg, Warren, & Beebe, 2015; Woods & Allspaw, 2020). Gaining a better understanding of hacker personality differences could help identify potential attack methods and improve defensive strategies (Basak et al., 2018; Curtis et al., 2021; Jones et al., 2021).

Although the technical details of known cyber threats are well documented and continually studied, the personalities of attackers are rarely understood (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020). Addressing this gap may strengthen cyber defenses and open new avenues for research into the traits of this elusive group (Basak et al., 2018; Curtis et al., 2021; Jones et al., 2021).

Preventing cyber-attacks requires attention to the personality traits and behavioral choices of cyber threat actors (Gaia et al., 2020). Examining personality traits can provide valuable insights to support proactive strategies for mitigating cybersecurity risks and threats. Therefore, this study focused on personality traits within the Big Five and the Dark Triad, as well as their relationship to intrusion behaviors and decision-making throughout the cyber-attack lifecycle. The study investigated how personality traits predict cyber intrusion behaviors.

Background

Cyber-attacks are estimated to occur every 30 seconds, with more than 2,000 occurring each day (Fox, 2023; Gaia et al., 2022). The rate of cyber-attacks has increased over the past 50

years, with a 75% year-over-year rise in cloud environment intrusions in 2023 alone (CrowdStrike, 2024). Threat actors have become highly focused on attacking critical infrastructure, as its compromise can cause significant harm to society and the economy (eSentire, 2023; Fox, 2023; U.S. Department of Homeland Security, 2024).

The cost of cyber-attacks and data breaches has soared to unprecedented levels, resulting in organizations incurring substantial financial losses, often amounting to millions of dollars after a single attack (Gaia et al., 2020; IBM, 2023). The aftermath of a major cyber-attack and data breach typically leads to higher prices or forces companies to shut down because they cannot recover from the financial damage (eSentire, 2023; Gaia et al., 2020; IBM, 2023).

In 2022, losses from cyber-attacks exceeded $10 billion, a 49% increase from the previous year (FBI Internet Crime Complaint Center IC3, 2023). Experts predict that global financial losses will go beyond $13 trillion by 2027 (eSentire, 2023; Fleck, 2024). Still, these numbers are based on reported cybersecurity incidents. Nearly 70% of organizations are believed not to report their incidents due to concerns about reputation and possible legal consequences (Gaia et al., 2021).

The increasing frequency and cost of cyber incidents have led organizations to allocate larger budgets to enhance their defenses and adopt more sophisticated security measures (Maxmillian & Sinha, 2022; Verizon, 2024). Many organizations have adopted a zero-trust framework, treating all applications, software, services, and individuals as untrusted until verified as reliable (Goasduff, 2023; IBM, 2024). Despite these advancements and process controls, the architecture of technical systems remains complex and often fragmented, weakening organizational resilience and creating significant vulnerabilities (DTEX i3, 2023; Verizon, 2022; Verizon, 2024; Woods & Allspaw, 2020).

The growing complexity in infrastructure, applications, and user behavior offers more opportunities for threat actors to exploit weaknesses. This situation has worsened due to an increase in critical vulnerabilities and zero-day exploits, fueled by greater interconnectedness and evolving work environments, such as remote and hybrid setups (Budimir et al., 2021; Khando et al., 2021; Kennison & Chan-Tin, 2021; Ma, 2021; Falowo et al., 2022; Pranggono & Arabo, 2020). Threat actors frequently discover and exploit technical flaws before security teams are aware, maintaining a strategic advantage (Verizon, 2023).

Cyber threat actors continually evolve their tactics, techniques, and procedures (TTPs), leveraging emerging technologies to enhance their attack capabilities (Sailio et al., 2020). Frameworks like MITRE ATT&CK (pronounced “attack”) adapt quickly as the security community detects and responds to new attack methods, offering an ever-growing catalog of adversarial behaviors (Al-Shaer et al., 2020; Deepwatch, 2024; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020; Strom et al., 2018). However, a key gap remains. The catalog of technical indicators shows what attacks do, but not who they are. Gaining deeper insight into attackers’ personalities and psychological motives, along with the TTPs they choose, could complement the framework and strengthen the human aspect of cybersecurity defenses (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Jones, 2022; Straub, 2020).

While the technical aspects of cyber-attacks are well-documented, the link between specific personality traits and the TTPs hackers use remains relatively unknown (Jones et al., 2021). Understanding how personality affects TTP selection is essential for equipping defenders with improved strategies, playbooks, and threat-detection methods, thereby enabling more proactive measures and faster detection and resolution times (Basak, 2018; Curtis et al., 2021; Jones et al., 2021).

Definitions

Understanding the distinctions between cyber threat actors, cyber-attacks, incidents, and data breaches is vital. Definitions of cybersecurity and cyber-attacks can often be vague and inconsistent because different organizations interpret these terms differently (Sailio et al., 2020). However, as Maxmillian and Sinha (2022) noted, it is important to recognize these differences, since each term pertains to a specific aspect of cybersecurity. The US National Institute ofStandards and Technology (NIST) is a leading authority on cybersecurity standards; therefore, this study will adopt the definitions and standards set by NIST (Sailio et al., 2020).

- **Cyber-attack** – Any malicious activity that attempts to obtain unauthorized access to technical systems and data, to access or steal data, cause a technical disruption to the system or organization, or degrade or destroy the data and information (NIST SP 800-12 Rev. 1).
- **Cyber Breach** - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar event where a person, other than an authorized user, gains access to, or potentially gains access to, sensitive information; or an authorized user accesses sensitive information for purposes other than those authorized (NIST SP 800-53 Rev. 5).
- **Cyber Incident** – Any event that affects the confidentiality, integrity, or availability of data, information, and technical systems, as well as any incident involving a violation or imminent threat of violating security policies, security procedures, or acceptable use policies (NIST SP 800-12 Rev. 1).
- **Threat Actor** – A person or group that presents a threat or causes harm (NIST SP 800-150). Threat actors are also known as hackers.

- **Tactics, Techniques, and Procedures (TTPs)** – defined by the MITRE ATT&CK Matrix - Tactics are seen as the "why" behind the attack, representing the goals and reasonsactingction. Techniques represent the "how" of the attack, explaining how an adversary acts. Procedures refer to the specific methods used to implement tactics and techniques.
- **Vulnerability** – Weaknesses within information systems, system security, controls, or implementation that a threat can exploit (NIST-SP 800-53 Rev. 5).

A cyber-attack is the overarching term for an event in which a threat actor maliciously targets the network or system of a specific organization or individual to steal, damage, or otherwise compromise data (Burton, 2023; NIST SP 800-12 Rev. 1). Cyber-attacks can be driven by various motivators, including, but not limited to, political, ideological, or financial gain (eSentire, 2023; Ma, 2021).

Cyber breaches and cyber incidents are often used interchangeably; however, they have distinct definitions. As described in NIST SP 800-53 Rev. 5, a cyber breach specifically aims to gain unauthorized access to sensitive technical information. This information can include Personal Information (PI), Personally Identifiable Information (PII), Protected Health Information (PHI), or a business's proprietary data. Such information can be useful for a threat actor, as it can be exploited to extort the victim, sold for profit, or shared with other entities for espionage or other illegal activities. Cyber breaches require organizations to disclose and report the breach to regulatory agencies (Burton, 2023; NIST SP 800-53 Rev. 5; Verizon, 2023). An incident is an event in which anattack succeeds, resulting in a loss of confidentiality, integrity, or availability of the targeted organization's data and information assets (NIST SP 800-12 Rev. 1;

Verizon, 2023). While these three terms are related, not every incident results in a cyber breach, although a breach is classified as a cyber incident (Burton, 2023; Verizon, 2023).

For this study, the term “threat actor” or "hacker" refers to the individual responsible for a potential cyber-attack, incident, or breach (Johnson, 2016). They often exploit technical vulnerabilities and weaknesses in systems (NIST SP-800-53 Rev. 5).

Problem Statement

The problem statement for the dissertation study is that while security practices and controls are crucial for protecting organizations, the extent to which the Big Five Personality Traits (Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) and the Dark Triad (Narcissism, Machiavellianism, and Psychopathy) influence cyber intrusion behaviors and decision-making practices remains unknown (Goldberg, 1993; Gaia et al., 2022).

The study aimed to explore the nuances and intersections of personality traits and cyber intrusion and hacking behaviors. Specifically, it examined how individual personality traits relate to the specific TTP choices made. The dissertation employed a mixed-methods approach, with participants completing both closed- and open-ended questions via a web-based survey platform. While this study is theoretical and exploratory, understanding how personality traits influence intrusion decision-making may have downstream relevance for cybersecurity practice. Specifically, insights into dispositional tendencies associated with personality, deception, or risk tolerance could help inform future approaches to cybersecurity training, insider-threat detection and mitigation, and the interpretation of adversarial behaviors beyond purely technical indicators.

Significance of the Study

Cybersecurity research has historically focused on technical systems, tools, and vulnerabilities, often considering human behavior as secondary or merely contextual. This study enhances the field by highlighting the importance of individual personality differences as key factors in cyber intrusion decision-making. By combining insights from personality psychology with cybersecurity, this approach deepens understanding of how cognitive styles, motivations, and dispositional traits influence intrusion behaviors beyond technical skills alone.

The results are important for both academic research and practical application. Theoretically, this study advances cybersecurity knowledge by empirically connecting the Big Five and Dark Triad personality traits to intrusion behaviors through a mixed-methods approach. Combining quantitative analysis with qualitative insights offers a detailed understanding of how personality affects not just the choice of tactics but also how individuals adapt, persist, and rationalize their decisions in an intrusion context.

From an applied perspective, this study offers initial insights that could guide future cybersecurity training, workforce development, and defensive strategies. Understanding how traits linked to persistence, deception, creativity, and risk tolerance influence intrusion decision-making can help organizations better interpret adversarial behavior, improve insider threat detection, and develop stronger, proactive cybersecurity strategies. Moreover, the research may support workforce development by equipping personnel with ethical decision-making and self-regulation skills alongside technical training. Although the findings do not offer specific prescriptions, they underscore the importance of integrating human-centered and personality-based approaches into cybersecurity research and practice.

Scope

This mixed-methods, non-experimental study investigated the relationship between Big Five personality traits (Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) and the Dark Triad (Narcissism, Machiavellianism, and Psychopathy). It also examined how these traits relate to preferred methods of cyber intrusion. The researchers used the MITRE ATT&CK Framework to analyze attack tactics and techniques across attack stages and to examine how participants' personalities influenced their decision-making.

The research used an online survey that included the Big Five and Dark Triad questionnaires, along with open-ended questions about TTP choices during a simulated cyber-attack. Participants were recruited from various online cybersecurity forums and platforms, including Discord and Reddit.

Quantitative data consisted of participants' personality profiles, whereas qualitative data were obtained from open-ended, Tabletop Exercise-style questions that emphasized decisions and tactics selected across various MITRE ATT&CK phases. The MITRE ATT&CK Framework was subjected to deductive content analysis and organized into a codebook for further study. Once responses were gathered, each open-ended answer was examined and linked to the self-reported personality inventory.

This study explored how individuals make decisions during simulated cyber intrusions. Human participants took part in a tabletop exercise set in a mock hospital environment, which included details about the time of year, organizational structure, and technical layout. The focus was on understanding how personality traits affect reasoning and behavioral intentions in hypothetical intrusion scenarios, rather than analyzing real-world cyber-attacks.

The study did not examine nation-state threat actors, organized cybercrime groups, or advanced persistent threat (APT) campaigns. Instead, it focused on individual cognitive and

behavioral decision-making, regardless of participants' roles as cybersecurity professionals, students, or hobbyists. Recruitment was limited to publicly accessible platforms to avoid ethical, legal, and safety concerns associated with illicit or covert cybercrime communities. The research did not cover organizational dynamics, team-based attack coordination, or geopolitical motivations.

Additionally, the research did not attempt to assign specific tactics to real-world threat actors, predict actual attack outcomes, or evaluate the effectiveness of technical exploits. The findings should be viewed as indications of general tendencies and thought processes in a simulated environment, not as precise indicators of real-world cyber intrusion activities.

Research Questions

Primary Research Question (RQ1): Do the Dark Triad personality types (narcissism, Machiavellianism, and psychopathy) influence individuals' decision-making processes when selecting specific tactics, also referred to as adversary tactical goals, for cyber-attacks?

Supporting Research Question (RQ2): Do the Big Five personality traits (Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) correlate with cyber intrusion behaviors?

Hypotheses

Primary Hypothesis

Hypothesis 1

Individuals scoring high on Dark Triad traits will favor bold, deceptive, and high-risk techniques.

This hypothesis aligns with Research Question 1 and serves as the study's central focus. It posits that individuals with elevated Dark Triad traits are more likely to engage in high-risk and deceptive behaviors, such as privilege escalation, lateral movement, and evasion tactics, particularly when encountering resistance or detection during an intrusion scenario.

Sub-questions supporting Hypothesis 1

Are certain Dark Triad traits more strongly predictive of specific adversary tactics (e.g., lateral movement, privilege escalation)?

Do individuals high in Dark Triad traits demonstrate greater persistence despite detection or countermeasures?

How do high Dark Triad scorers differ in their preferred attack vectors when compared to low scorers?

Supporting Hypotheses: Big Five Personality Traits

These hypotheses support Research Question 2, which explores how standard personality dimensions contribute to or moderate intrusion decision-making.

Hypothesis 2

Individuals high in Openness and low in Neuroticism will favor creative and sophisticated intrusion techniques.

This hypothesis posits that cognitive flexibility, curiosity, and tolerance for ambiguity support exploratory and adaptive intrusion strategies.

Hypothesis 3

Individuals high in Conscientiousness will prefer structured, low-risk approaches to network intrusion.

This hypothesis is grounded in personality theory linking Conscientiousness to planning, discipline, and procedural adherence, which are expected to manifest as organized, phased intrusion behaviors.

Hypothesis 4

Individuals high in Extraversion are more likely to use Social Engineering tactics.

This hypothesis reflects the association between Extraversion, confidence, and interpersonal engagement, which may facilitate human-centric manipulation and direct interaction during intrusion attempts.

Hypothesis 5

Individuals low in Agreeableness and Neuroticism will tend to employ more aggressive intrusion methods.

This hypothesis is supported by prior research linking low Agreeableness to competitiveness, reduced concern for social norms, and increased tolerance of adversarial behavior.

Limitations

The primary limitation of this study is reliance on self-reported personality data. Although the Big Five Inventory and the Short Dark Triad Scale are well-validated and widely used instruments, self-reported measures are inherently susceptible to social desirability bias and

inaccurate self-assessment. Participants may underreport socially undesirable traits or overemphasize characteristics aligned with professionalism and competency, potentially affecting the precision of trait measurement. Although anonymity and careful study design were used to mitigate these effects, self-report bias remains a threat to internal validity.

A second limitation concerns the use of a simulated tabletop intrusion scenario rather than observing real-world intrusion behavior. Participants were asked to describe how they would respond to a cyber intrusion under hypothetical conditions, rather than engage in live attacks with real operational, legal, or ethical consequences. As a result, stated intentions may differ from actual behavior under conditions involving time pressure, detection risk, or organizational accountability. Although the scenario was designed to mirror realistic attack phases using the MITRE ATT&CK Framework, this distinction limits the direct behavioral generalizability of the findings.

The study's sampling approach also limits generalizability. Participants were recruited from public online communities and primarily consisted of cybersecurity professionals, students, and technically inclined individuals. The findings may therefore not generalize to nation-state actors, organized cybercrime groups, or individuals operating within closed or illicit networks, where motivations, norms, and constraints may differ substantially. The study intentionally focused on individual-level decision-making rather than coordinated groups or geopolitical threat behavior.

The cross-sectional design limits conclusions about causality or developmental change. Personality traits and intrusion behaviors were measured at a single time point, preventing assessment of how these relationships may evolve, with experience, or across changing situational contexts.

Finally, although several personality traits showed statistically meaningful associations with intrusion behaviors, the observed effect sizes were generally modest. This reflects the complex, multifactorial nature of cyber intrusion decision-making, in which personality is one of many contributing influences, including situational factors, technical constraints, and environmental opportunities. The findings should therefore be interpreted as identifying dispositional tendencies rather than deterministic predictors of behavior.

Delimitations

This study involved several deliberate design choices that limited the scope to ensure feasibility and alignment with the research questions.

Participants: The sample was deliberately restricted to individuals with experience or interest in cybersecurity-related domains, including ethical hacking, penetration testing, and information security. Participants were recruited through online forums, Discord servers, and cybersecurity-focused communities. Individuals without a background or engagement in cybersecurity were excluded, as the study aimed to examine intrusion decision-making among those familiar with technical attack concepts.

Language Proficiency: All survey instruments and the scenario-based tabletop exercise were administered exclusively in English. No translation tools or multilingual versions of the instruments were provided. This limitation was necessary to ensure consistent interpretation of items, particularly for technical terminology, but it limits participation to English-proficient respondents.

Tactical Scope: The scenario-based tabletop exercise was intentionally limited to six MITRE ATT&CK tactics: Reconnaissance, Initial Access, Execution, Defense Evasion, Persistence, and Privilege Escalation. These tactics represent the early-to-mid stages of cyber

intrusions, where individual decision-making and personality influences are most salient. Later-stage tactics, such as Command and Control, Exfiltration, and Impact, were excluded to reduce cognitive load, prevent participation fatigue, and maintain analytic focus on strategic planning and adaptive behavior.

Summary

Understanding the motives behind a threat actor's cyber-attack has become essential in cybersecurity efforts. Experts recommend moving beyond purely technical safeguards and instead focusing on understanding the different types of individuals likely to engage in malicious activities (Burton, 2023; Shackelford et al., 2023).

Many criminologists recognize that while an organization's technical infrastructure and security controls can provide some protection against cyber threats, no system is entirely immune, and attacks still happen frequently (Al Shraah et al., 2021). To grasp attackers' changing tactics, experts highlight the need to examine threat actors' personality traits and understand decision-makers' minds (Diesch et al., 2020; Haz et al., 2022; Jones et al., 2021; Selzer & Oelrich, 2021). Using psychology in crime prevention is not a new approach; psychologists and mental health specialists have collaborated with law enforcement to spot patterns, behaviors, and personality traits that can enhance preventative efforts against malicious, harmful, or illegal activities (Haz et al., 2022; Selzer & Oelrich, 2021). Researchers have identified notable behavioral patterns associated with criminals based on the Big Five Personality Traits and the Dark Triad, which may be crucial for understanding cyber-attack and intrusion behaviors.

Most criminologists agree that threat actors possess both hard and soft skills, underscoring the key role of personality in malicious cyber activities (Chng et al., 2022; Gaia et

al., 2021; Papatsaroucha et al., 2021). The Big Five and Dark Triad models are often considered useful for identifying individuals more likely to commit illegal acts (Bolelli, 2020; Curtis et al., 2021; Kiire et al., 2020; Ock, 2023). However, research on the specific personality profiles of cyber threat actors and their hacking techniques remains limited (Harms et al., 2022; Ock, 2023). Scholars emphasize the need for detailed studies of cyber threat actors, particularly how personality traits may influence hacking and intrusion behaviors (Harms et al., 2022; Ock, 2023). Understanding the link between personality and decisions about network intrusions could help organizations develop better prevention and defense strategies.

The research outlined in this chapter examined the relationships among the Big Five Personality Traits, the Dark Triad, and hacking, intrusion practices, and decision-making. The study took place amid a surge in cyber-attacks and data breaches, exploring the psychological profiles of individuals who self-report involvement in hacking or intrusion activities. It critically examined whether traits associated with the Big Five Personality Traits and the Dark Triad are linked to hacking behaviors. This research is essential for understanding the complex interplay between personality traits and cybersecurity risks and may yield new insights beyond traditional security measures. Additionally, the study aimed to contribute to the development of more effective cybersecurity strategies by investigating the psychological aspects of cybercrime, with a focus on understanding and, if possible, reducing the human factor in hacking incidents.

LITERATURE REVIEW

The cyber threat landscape is constantly evolving, with threats becoming more sophisticated, innovative, and complex (Jones et al., 2021; Maxmillian & Sinha, 2022; Romanosky & Boudreaux, 2021; Verizon, 2024). These systems are highly interconnected, handling large volumes of data from various sources, making them challenging to implement and manage. This complexity has significant security implications for organizations (Ma, 2021; Olufunsho, F. et al., 2022; Povše, 2019; Romanosky & Boudreaux, 2021). Moreover, many organizations struggle with employees not consistently following strong security practices on their devices and within systems (Ahmad et al., 2019). While technical and organizational vulnerabilities help identify potential threats, they only provide part of the full picture. To thoroughly understand the cyber threat environment and how cyber-attacks unfold, it is crucial to consider the individuals behind these attacks and the psychological factors that influence their behavior.

Motivations for cyber-attacks are complex, but personality remains an important factor in understanding hacker behavior beyond surface-level incentives. One well-established driver is the increasing value of targeted data, as the monetization of sensitive information, such as Personally Identifiable Information (PII) and other protected data (like health records or financial information), in the cybercrime underground has grown, leading attackers to focus on acquiring and exfiltrating data (IBM, 2023). Although attackers may be motivated by status or financial gain, analyses of attackers often overlook the role of personality types in shaping how these motivations turn into specific behaviors (Georgiadou et al., 2021; Petry, 2011).

Frameworks such as MITRE ATT&CK provide detailed technical information on attack tactics and techniques, offering critical value to threat intelligence and incident responders

(Georgiadou et al., 2021; Petry, 2011; Verizon, 2022). However, these frameworks mainly focus on how cyber-attacks occur, emphasizing the technical aspects of attribution. Understanding the persona behind the attack remains unclear. Gaining insight into hackers' psychological and behavioral traits can complement technical knowledge and help develop more proactive and preventive countermeasures (Georgiadou et al., 2021; Petry, 2011; Verizon, 2022).

The problem addressed in this study is that, despite a high number of cyber-attacks, how personality traits influence the behaviors and decision-making processes of threat actors remains unknown (CrowdStrike, 2023; IBM, 2023; Harms et al., 2022; Verizon, 2023). This study aimed to help bridge the research gap (Harms et al., 2022). Therefore, the goal of this mixed-methods, non-experimental research was to examine the relationships between the Big Five (Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) and the Dark Triad (Narcissism, Machiavellianism, and Psychopathy) to understand how these traits relate to intrusion practices.

MITRE ATT&CK Framework

The MITRE ATT&CK Framework (ATT&CK, standing for Adversarial Tactics, Techniques, and Common Knowledge) is widely regarded as an industry-standard repository of threat actor and adversary tactics, techniques, and procedures, also known as TTPs (Georgiadou et al., 2021; Strom et al., 2018; Verizon, 2022). The framework is built on documented real-world attacks, giving defenders the intelligence they need to safeguard networks and illustrating that attacks are persistent and highly sophisticated (Deepwatch, 2024; Strom et al., 2018). The comprehensive knowledge within the framework aims to model threat actors' technical methods, helping defenders anticipate potential attacks before they occur (Belfadel et al., 2022). While the repository contains extensive technical details, it lacks insights into the behavioral and

personality traits of the humans behind the attack TTPs (Al-Shaer, Spring, & Christou, 2020; Georgiadou et al., 2021).

The framework is built around five key elements for every threat: tactics, techniques, sub-techniques, procedures, and mitigations for defenders (Georgiadou et al., 2021). As Georgiadou et al. (2021) explain, tactics refer to the strategic purpose of an attack, or the "why." Tactics provide important context for understanding different types of potential threats (Strom et al., 2018). Techniques clarify the attacker's goals by describing the "how" and "what" they aim to achieve, with sub-techniques offering more detailed insights into the technical behaviors involved (Georgiadou et al., 2021; Strom et al., 2018). Procedures outline the specific steps for carrying out techniques, such as using an executable to dump credentials (Strom et al., 2018). Mitigations are the countermeasures defenders can deploy to respond to threats. Information about each tactic within the framework helps to understand better the attacker's strategic goals and potential methods of execution (Al-Shaer, Spring, & Christou, 2020).

Understanding TTPs can help with attribution, as they are often considered key indicators of a specific threat actor's identity (Warikoo, 2021). Indicators of Compromise (IoCs) are technical signatures used to identify malicious activity within a network (Strom et al., 2018). IoCs are essential for understanding attack operations, providing defenders with actionable intelligence to hunt for signs of compromise in their networks (Strom et al., 2018).

MITRE ATT&CK is a comprehensive catalog that continually expands as new attack techniques are discovered. The framework's scope depends on incident reports, community research, and information-sharing datasets (Strom et al., 2018). However, there are gaps in understanding cybersecurity threats, particularly regarding a complete picture of the attacker behind the attack (Al-Shaer, Spring, & Christou, 2020).

Attack potential is evaluated using technical factors recognized by the cybersecurity community and based on industry standards and frameworks such as the U.S. National Institute of Standards and Technology (NIST) and MITRE ATT&CK (Kioskli & Polemi, 2020; Sailio et al., 2020). These standards and frameworks are vital for cybersecurity defenses, as threat intelligence enables proactive strategies to adapt to the constantly evolving threat environment (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020; Verizon, 2022). Cyber-attacks are becoming more sophisticated, posing challenges for defenses and highlighting the importance of strengthening cyber protections (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020; Verizon, 2022).

Managed Security Service Providers (MSSPs) often publish reports on the most common attack techniques observed in recent months or years (Deepwatch, 2024). For instance, MSSPs frequently alert the community about the use of valid accounts, brute-force attacks, modifications of system processes, and other prevalent TTPs. Cyber-attacks often follow a multi-phase approach, in which the threat actor conducts reconnaissance on the target, then proceeds through weaponization, delivery, exploitation, network control, execution, and maintenance (Al-Shaer, Spring, & Christou, 2020; Straub, 2020). While this information is valuable for defenders, a lack of understanding of the attacker behind the attack remains a known gap. Without a clear grasp of the individual's personality and how it relates to intrusion methods, we cannot determine how attackers might combine TTPs to develop and deploy new attack types (Al-Shaer, Spring, & Christou, 2020; Georgiadou et al., 2021; Straub, 2020).

Most organizations face a significant resource gap, as they need more time, skilled personnel, and financial backing to acquire comprehensive toolsets and threat intelligence feeds. This limitation hampers their ability to effectively defend against the ever-evolving landscape of

cyber threats (Maxmillian & Sinha, 2022; Verizon, 2024). Traditional security measures like firewall filtering, anti-malware, and virus scanning are no longer sufficient on their own (Liu et al., 2020; Wang & Liu, 2023). While these methods can mitigate some basic threats, they tend to be static and passive, leaving networks exposed to advanced and sophisticated attacks (Dang, 2023; Liu et al., 2020; Hu et al., 2020; Sengupta et al., 2020). To combat modern cyber threats effectively, defense strategies must be flexible and proactive, yet they often rely on after-the-fact incident analysis and technical indicators, which limit comprehensive and preventive measures (Al-Shaer et al., 2020; Georgiadou et al., 2021; Hu et al., 2020; Liu et al., 2019; Jones et al., 2021; Straub, 2020; Verizon, 2022).

Technical security controls are crucial for effective defenses; however, they often overlook the human element, leaving an important aspect unaddressed (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Straub, 2020; Verizon, 2022). To respond effectively to the changing technical landscape of cyber threats, it is important to consider the person behind the attack, as this will improve our understanding of the tactics used to initiate and execute an attack (Basak, 2018; Curtis et al., 2021; Jones et al., 2021; Jones, 2022; Kioskli & Polemi, 2020). Moreover, understanding the human element enables better predictions about potential targets at both the individual and organizational levels (Basak, 2018; Curtis et al., 2021; Jones et al., 2021; Jones, 2022; Kioskli & Polemi, 2020).

While “tried-and-true” attack methods continue to be employed and remain effective, many attackers are creating innovative approaches that require defenders to adapt their strategies (Verizon, 2024). A thorough understanding of the threats and the people behind them is crucial for proactive prevention, detection, and mitigation (Gaia et al., 2020; Jones et al., 2021; Jones, 2022; Ma et al., 2023).

Hacker Typology

The choice to remain stealthy while another chooses loud, aggressive TTPs is attributed to unique personality traits and intrinsic motivations (Jones et al., 2021; Garcia & Moraga, 2017). Various characteristics may contribute to hacking behaviors, including seeking attention, feelings of entitlement, an inflated sense of self, or lack of empathy (Garcia & Moraga, 2017; Jones et al., 2021; Jones, 2022; Maasberg et al., 2020). One's unique traits may provide insight into the tendency toward specific hacking behaviors (Curtis et al., 2021; Jones et al., 2021). For instance, someone may be cautious, choose to hide in plain sight, and gradually exfiltrate data over an extended period to avoid detection due to heightened anxiety levels (Curtis et al., 2021; Jones et al., 2021). Others, displaying lower levels of anxiety, may be conspicuous in their actions, generating significant noise, triggering security alarms, and quickly exfiltrating large volumes of data (Curtis et al., 2021; Jones et al., 2021). Despite these opposing behaviors, the choice to act in a particular manner reflects the individual personality traits that drive their TTP selections (Curtis et al., 2021; Jones et al., 2021).

Many factors shape the intersection of personality and hacking behavior. The fear of detection may deter some individuals from engaging in easily detectable hacking activities (Jones et al., 2021). Others may be motivated to remain within a network longer to inflict greater-scale damage or breach other organizational networks via supply-chain attacks (Jones et al., 2021). Certain personality traits, particularly those linked to the Dark Triad, may lead to a preference for easily detectable or "noisy" methods, as these individuals often experience little anxiety and may ignore the alerts they generate (Jones et al., 2021). However, personality is a multifaceted construct and does not always provide a straightforward explanation for specific behaviors (Garcia & Moraga, 2017; Hudson, 2022).

To comprehend hackers' personality profiles and their decision-making processes, understanding hacker typology, comprising white, gray, and black hats, is crucial (Gaia et al., 2020). As shown in Table 1, typology is based on motives and intentions (Gaia et al., 2020). While all three types exhibit similar behaviors, their core motivations differ, making it important to recognize these distinctions. However, research exploring the detailed differences among hacker types remains limited (Gaia et al., 2020; Gaia et al., 2022).

Table 1.

Breakdown of Hacker Typology

Typology	Definition
White Hat	Ethical hackers are often viewed as "the good guys" who hack for their profession (Gaia et al., 2020; Amo et al., 2023; Kumawat et al., 2023; Thomas et al., 2019; Wang et al., 2017).
Grey Hat	Hacktivists, or those who are driven by ideological motivations (Gaia, 2020; Gaia et al., 2021).
Black Hat	Those whose hacking is to cause damage or harm (Banda et al., 2019; Gaia et al., 2020; Gaia et al., 2021; Lazarov & Petrova, 2022; Rosenbaum, 2010; Wang et al., 2017; Xu & Zhang, 2013).

White Hat

White hats are often referred to as ethical hackers or "the good guys," hack professionally or to address technical issues (Gaia et al., 2020; Amo et al., 2023; Kumawat et al., 2023; Thomas et al., 2019; Wang et al., 2017). These individuals occupy roles like penetration testers, which stand in stark contrast to the typical dark image of hackers often portrayed in the media (Kumawat et al., 2023; Lazarov & Petrova, 2022). These individuals are legally authorized to identify, test, and resolve potential security concerns to enhance organizational security (Amo et

al., 2023; Kumawat et al., 2023; Thomas et al., 2019; Wang et al., 2017). Organizations often engage white hat hackers to assess their security systems and identify gaps or vulnerabilities in their technical environment that threat actors could exploit (Kumawat et al., 2023). Testing the technical infrastructure and systems strengthens the organization's security posture (Kumawat et al., 2023). White hat hackers employ the same tools and methodologies as threat actors, but they aim to detect and mitigate security vulnerabilities. Because their actions are authorized, these behaviors are legally acceptable (Amo et al., 2023; Kumawat et al., 2023).

Grey Hat

Grey hat hackers are often referred to as "hacktivists" (Gaia, 2020; Gaia et al., 2021). They are typically motivated by ideology, believing they are opposing practices they consider wrong or harmful (Gaia, 2020; Gaia et al., 2021). Their typical targets include politicians, government entities, celebrities, and large organizations (Gaia, 2020; Gaia et al., 2021).

Grey hats are often more ambiguous about their ethical considerations, with motivations that are not fundamentally malicious but may involve breaking the law to achieve their objectives (Lazarov & Petrova, 2022). They are distinguished from white hats by their "irregular compliance with the laws to reach their objectives" (Lazarov & Petrova, 2022). Additionally, grey hats differ from black hats in that their motivations are not driven by greed and financial gain, but rather by a desire to take a stand against those they oppose (Lazarov & Petrova, 2022).

Black Hat

Black hat hackers are individuals who exploit systems for personal or financial benefit, motivated by greed and malicious intent (Banda et al., 2019; Gaia et al., 2020; Gaia et al., 2021; Lazarov & Petrova, 2022; Rosenbaum, 2010; Wang et al., 2017; Xu & Zhang, 2013). These

hackers are motivated by the thrill, financial benefit, or the desire to cause significant disruptions for nefarious purposes (Banda et al., 2019; Gaia et al., 2020; Gaia et al., 2021; Lazarov & Petrova, 2022; Rosenbaum, 2010; Wang et al., 2017; Xu & Zhang, 2013). Black hat hackers are commonly associated with the traditional image of a "hacker" (Lazarov & Petrova, 2022). They are often seen as seeking revenge, engaging in sabotage, committing theft, and aiming to inflict substantial damage (Gaia et al., 2021; Lazarov & Petrova, 2022; Xu & Zhang, 2013). Typically, black hat hackers are indifferent to the legality of their actions, focusing instead on the notoriety and personal gain associated with their attacks (Banda et al., 2019; Gaia et al., 2021).

Typology Complexities

Understanding the differentiation among hacking typologies is complex because hacker categories are not mutually exclusive; an individual can engage in multiple types of hacking behavior over their lifetime or even concurrently (Gaia et al., 2020; Thomas et al., 2018). This largely depends on personality traits, motivations, and opportunities (Gaia et al., 2020; Thomas et al., 2018). Hacking behavior evolves; a person might start as a white hat hacker and, over time, transition into black hat hacking as they acquire experience and advanced skills (Thomas et al., 2018). Conversely, some individuals may begin their careers as black hat hackers and eventually move into ethical hacking, using their skills to contribute positively to cybersecurity (Thomas et al., 2018). Hacking typologies can also operate in parallel; a person might hack within ethical and approved boundaries in their day job but disregard their moral principles to hack for ideological or nefarious reasons outside of their professional responsibilities (Gaia et al., 2020; Thomas et al., 2018). Understanding hacking typology is crucial because the motivations behind hacking interact with personality types and behaviors.

Personality

Defining personality is complex and often debated (Allman, 2018; Bergner, 2020). The American Psychological Association (2025) describes personality as the enduring traits and behaviors that shape an individual's unique way of adjusting to life, including key traits, interests, drives, values, self-concept, abilities, and emotional patterns. They further explain that while personality develops through various processes, a person's distinctive traits primarily influence their behaviors.

Personality is a vital framework for understanding behavior, how individuals engage with their surroundings, and how they navigate situations. Investigating personality involves understanding how distinct characteristics shape interpersonal relationships, influence decision-making, and affect one's unique responses (Ashton, 2022). Specific terms used to describe personality do not directly reflect biological or psychological processes; instead, they are socially constructed labels that represent observable behavioral patterns (Ashton, 2022). However, trait naming is often criticized because, while it offers convenient ways to describe one's personality, it does not capture the entirety of an individual or their behavioral choices (Ashton, 2022).

Personality is often considered intricate and relatively stable throughout one's lifespan. However, research indicates that it can be dynamic, with traits not regularly present manifesting in certain situations (Ashton, 2022). Intrinsic characteristics and external factors, such as one's environment or life experiences, can also shape which traits emerge (Ashton, 2022; Gaines, 2019). For instance, environmental situations, such as highly stressful events, can lead to the manifestation of specific traits, while other characteristics remain stable (Ashton, 2022).

Personality is a foundational concept in psychology, and individual personality typology is categorized into broad dimensions (Gosling et al., 2003). Researchers have struggled to reach consensus on the core dimensions of personality (John et al., 2008). Critics frequently argue that

grouping traits oversimplifies the range of traits and overlooks other factors, such as situational influences and dynamic processes (Bergner, 2020; Roberts & Yoon, 2022).

Personality is the basis for understanding human variability and for identifying individual differences. The field not only examines the nature of personality but also explores its development, including the construction of traits, population variations, the understanding of enduring, stable differences, and maladaptive personality traits (American Psychological Association, 2025). Psychologists and other professionals in the field often debate trait classifications; however, it is argued that most individuals perceive descriptive characteristics as representative of one's personality, a phenomenon referred to as trait naming (Allman, 2018; Allport & Odbert, 1936).

Scientific approaches to personality have evolved significantly, embracing diverse methodologies and theoretical frameworks to understand the complexity of traits, behaviors, and cognitive patterns that define individuals (Ashton, 2022; Mischel & Shoda, 1995). Given its central role in shaping behavior, personality research provides critical insights into why individuals act as they do across contexts, including in the digital environment.

Historical Perspectives of Personality

Personality has been studied throughout history to understand what makes individuals unique. Although they did not directly research personality, philosophers such as Aristotle and Plato are often credited with laying the groundwork for contemporary trait naming conventions, including ideas about Conscientiousness and emotional stability (John et al., 2008; Matulessy & Humaira, 2016).

Kernberg (2016) notes that the DSM-5's classification of personality disorders lacks integration of the self and relationships with others. This integration aligns with the philosophical

perspective that a unified understanding of the self is essential to understanding why people behave as they do (Kernberg, 2016). These historical findings provided a foundational framework for subsequent scientific efforts to assess and categorize personality traits systematically (Ashton, 2022; John et al., 2008).

Early researchers often examined the interplay between traits and behavioral patterns, as well as the unique ways individuals perceive their environment (Gaines, 2019). Researchers like J.P. Guilford pioneered trait naming and factor analysis to identify major characteristics within one's unique personality set (Gaines, 2019). This led to the development of trait surveys, enabling many researchers to create robust tools for assessing personality (Gaines, 2019).

Trait naming and surveying have substantially refined over time (Ashton, 2023). Early work by researchers, such as Allport and Odbert (1936), compiled approximately 4,500 adjectives to describe personality. However, researchers identified conceptual and descriptive overlaps among the traits (Ashton, 2022). Researchers began organizing traits into broader, more manageable categories (Ashton, 2022; McCrae, 1991). This reduced redundancy and enhanced the efficacy and reliability of personality assessments (Ashton, 2022; McCrae, 1991). Historical perspectives of personality reflect observation and rationalism, which aim to distill complex human behaviors into quantifiable constructs (Gaines, 2019).

Stability of Personality

Over time, research has shown that personality remains relatively stable, especially in adulthood. However, life events, environmental influences, and other psychological factors can lead to changes and variations in personality traits (Guekes et al., 2018). Factors such as genetics, environment, cultural norms, life experiences, and social circumstances are believed to influence both the specific traits someone displays and their stability (Guekes et al., 2018). The

dynamic interaction between heredity and environment highlights the complexity of individual differences (Ashton, 2022). Personal characteristics and experiences also affect the stability of certain traits (Geukes et al., 2018; Kernberg, 2016).

The role of individual personality differences is fundamental to understanding human behavior and psychological traits (Ashton, 2022). These differences are shaped by factors throughout an individual's lifespan (Ashton, 2022). As people age, specific characteristics, such as Agreeableness, tend to increase due to developmental changes and the adoption of social roles (Ashton, 2022). For instance, patience and flexibility often become more pronounced as individuals navigate life experiences that demand adaptability and interpersonal harmony (Ashton, 2022).

As previous research indicates, numerous factors can influence personality, suggesting that individual trait patterns can evolve (Ashton, 2022). This idea challenges the traditional view that personality traits are fixed and unchanging, suggesting instead that a variety of internal and external influences can drive trait development (Ashton, 2022). Although studies demonstrate that personality traits generally remain stable, they are not entirely resistant to change; such changes can happen gradually throughout a person's life or quickly following a significant life event or external factor (Ashton, 2022).

The debate surrounding the existence of traits as stable parts of personality has been extensive. While situational factors play a crucial role, research shows that people exhibit behavioral variation across contexts (Ashton, 2022). This bolsters the idea that traits are essential aspects of personality. Researchers have used statistical methods, such as analysis of variance, to investigate interactions between individuals and their situations, demonstrating how situational cues can elicit specific behaviors while preserving stable underlying traits (Ashton, 2022).

However, based on the potential for trait manifestation, it is crucial to adopt a dynamic approach to understanding and researching personality (Ashton, 2022).

Personality of Hackers

Personality research has become essential for understanding specialized populations, particularly within cybersecurity. In recent years, researchers have applied established personality frameworks to examine behavioral tendencies associated with hacking and cyber intrusion. Models such as the Big Five and the Dark Triad have proven valuable for identifying patterns of behavior related to rule-breaking, manipulation, and nonconformity, traits often linked to individuals who engage in unauthorized system access or socially disruptive activities online (Paulhus & Williams, 2002).

Understanding personality patterns is critical for understanding and anticipating cyber intrusion behavior (Basak et al., 2018; Ceccato et al., 2017; Jones, 2022; Ma, 2023). While the technical mechanics of cyber-attacks are well documented, psychological and behavioral dimensions remain comparatively underexplored (Al-Shaer et al., 2020; Georgiadou et al., 2021; Jones et al., 2021; Jones, 2022; Straub, 2020). Addressing this gap can improve defensive strategies, strengthen threat attribution, and reduce the effectiveness of cyber-attacks through a more comprehensive understanding of attacker behavior.

Prior research has employed the Big Five Personality Traits to examine psychological factors in computer science and cybersecurity (Papatsaroucha et al., 2021; Shappie et al., 2020). Threat actors are often portrayed as highly skilled yet antisocial, and some studies link them to traits associated with deviant behavior (Matulessy & Humaira, 2016). However, societal perceptions of hackers are heavily influenced by media portrayals that emphasize dysfunction

and malicious intent, reinforcing negative stereotypes that may not fully reflect empirical findings (Romanosky & Boudreaux, 2021; Warikoo, 2021).

Although white, grey, and black hat hackers are typically categorized by distinct characteristics, prior research indicates that they share several underlying personality traits (Abbott, 2019; Black, 2022; Gaia et al., 2022; Paulhus & Williams, 2002). Across these groups, elevated levels of Machiavellianism and Psychopathy from the Dark Triad have been observed (Gaia et al., 2020; Gaia et al., 2022). At the same time, meaningful differences emerge; for example, white hat hackers tend to score higher on Openness and assertiveness than their grey or black hat counterparts (Gaia et al., 2020; Gaia et al., 2022). These findings suggest that ethical orientation alone does not fully capture behavioral tendencies within hacker populations.

Personality is a complex and dynamic system that requires more nuanced approaches than linear trait assumptions allow (Garcia & Moraga, 2017; Hudson, 2022). Individuals may share similar trait profiles yet express those traits in markedly different ways depending on situational context, motivation, and opportunity (Garcia & Moraga, 2017; Neumann et al., 2021). For instance, Extraversion is sometimes conflated with psychopathic tendencies, even though many extraverted individuals do not exhibit psychopathic behaviors (Garcia & Moraga, 2017). Research further indicates that individuals high in dark traits often display varied expressions of the Big Five, reinforcing the need for integrative rather than reductionist models of personality (Garcia & Moraga, 2017).

The limitations of purely technical or categorical approaches are evident in real-world attribution efforts. In 2016, the Democratic National Committee (DNC) experienced a network intrusion that resulted in a high-profile cyber breach (Romanosky & Boudreaux, 2021). Although technical indicators were used to attribute the attack to actors associated with the Russian

government, the publicly released reports relied on ambiguous evidence, prompting criticism from cybersecurity professionals regarding the confidence in attribution and transparency (Romanosky & Boudreaux, 2021). This case highlights the difficulty of inferring intent, identifying actors, and determining motivations from technical artifacts alone, underscoring the need for complementary psychological and behavioral perspectives.

Taken together, existing research shows that hacker behavior cannot be adequately explained by technical indicators or categorical labels alone. Personality traits interact dynamically with situational factors to shape intrusion decision-making. This complexity motivates the present study's integrated framework, which combines the Big Five and Dark Triad models to examine how dispositional tendencies influence both the structure and intent of cyber intrusion behavior.

The Big Five Personality

The Big Five is a widely accepted inventory of personality traits and a framework for understanding human personality (Babcock & Wilson, 2020). This model categorizes personality into five broad dimensions: Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism (Matulessy & Humaira, 2016; Mammadov, 2022). The Big Five provides concise, comprehensive insight into the unique complexities of each individual's personality. The traits within the Big Five are orthogonal, meaning they are statistically independent; a high score on one trait does not necessarily predict a high score on another. This independence allows researchers to isolate personality dimensions to understand how these traits contribute to specific behaviors (Babcock & Wilson, 2020).

The Big Five Personality model originated from a pool of nearly 18,000 descriptive traits, which was considered a "semantic nightmare" in the 1930s (John, 2008). Over the years,

researchers reduced the list to a few thousand, and through extensive analysis, the traits were condensed into 16 core factors (John, 2008). In the 1980s, researchers further consolidated the identified traits into the Big Five (Ashton, 2022; John, 2008). The Big Five emerged as the dominant framework and gained significant traction as a reliable taxonomy for understanding personality (Ashton, 2022; John, 2008). The Big Five model holds that every individual possesses the five core traits to varying degrees, which together make up their unique personality (Mammadov, 2022).

The five dimensions, consisting of Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism, exist on a spectrum, where all individuals fall somewhere along the continuum for each trait (Zell & Lesick, 2022). Each person possesses varying degrees of the characteristics that collectively define their unique personality profile (Mammadov, 2022; Matulessy & Humaira, 2016; Zell & Lesick, 2022).

The traits represented in the Big Five are considered the foundation of individual differences among people (Goldberg, 1990). Although these traits are considered fundamental aspects of one's personality, they are not entirely fixed (Goldberg, 1993; Hudson, 2022; Matulessy & Humaira, 2016; Mammadov, 2022). Research suggests that traits are relatively stable throughout one's lifespan; however, they can change in response to life experiences, environment, and other factors (Uebelacker & Quiel, 2014). This dichotomy of stability and flexibility allows traits to be expressed differently depending on one's situation (Uebelacker & Quiel, 2014).

The five core traits within the Big Five capture distinct personality dimensions, providing a comprehensive framework for understanding individual differences (Goldberg, 1993). The nature in which traits are expressed on a continuum allows for an understanding of unique

personalities, where a person may exhibit high levels of some characteristics and lower levels in others individuals to exhibit high levels in some areas while being lower in others (Goldberg, 1993; Hudson, 2022; Matulessy & Humaira, 2016; Mammadov, 2022; Zell & Lesick, 2022). This highlights the individuality of personality (Goldberg, 1993; Hudson, 2022; Matulessy & Humaira, 2016; Mammadov, 2022; Zell & Lesick, 2022). The Big Five also acknowledges that it focuses on both positive and neutral aspects of personality; however, these core traits can become maladaptive when expressed at the extremes of the trait spectrum (Miao et al., 2023).

To better understand how these traits influence individual behavior, it is useful to define each dimension more precisely.

Openness traits are characterized by creativity, intellectual curiosity, and a fondness for novelty (Mamadov, 2022). Highly open people are typically imaginative, prefer new experiences, and are strong abstract thinkers (Bakas et al., 2021; Mammadov, 2022). In cybersecurity, this trait is often associated with black hat hackers; hackers who can demonstrate creative problem-solving skills, which enable them to adapt to new and emerging technologies and investigate and exploit technologies that may not have established hacking methodologies (Matulessy, 2016; Shappie et al., 2019). Regarding victimology, highly open people may be more vulnerable to specific attacks, such as phishing and ransomware (Cho et al., 2016; Yilmaz & Cetin, 2023).

Conscientiousness is reflected in self-discipline, organization, and goal-oriented behaviors. Highly Conscientious people typically are methodical, reliable, and effective at task management (Bakas et al., 2021; Matulessy & Humaira, 2016). Conscientiousness is often related to thoughtfulness, and these individuals tend to be highly driven and focused on their goals (Matulessy & Humaira, 2016). Within cybersecurity, low Conscientiousness is often

related to those who are more likely to engage in risky online behavior, whereas those who are highly Conscientious tend to follow best practices more closely and are less vulnerable to threats like phishing (Fagade et al., 2017; Frauenstein, 2021; Van de Weijer & Leukfeldt, 2017).

Extraversion is associated with socialability, energy, and assertiveness (Luo et al., 2023; Ji & Esqueda, 2022). Extraverted people tend to thrive in social environments. In cybersecurity, research has linked high Extraversion to a propensity for hacking, contradicting traditional hacker stereotypes (Bashir et al., 2017). Research also indicates that high Extraversion is associated with a greater risk of falling victim to cyber threats, such as phishing (Gerber et al., 2017; Frauenstein, 2021).

Agreeableness encompasses kindness, empathy, and a willingness to cooperate (Matulessy & Humaira, 2016; Soutter et al., 2020). Highly Agreeable individuals tend to have positive interpersonal relationships and demonstrate altruistic behaviors. In cybersecurity, prior research has indicated that high Agreeableness is linked to a greater likelihood of falling victim to Social Engineering attacks, while those who are less Agreeable tend to be more suspicious of others online, exhibiting less cooperative behaviors (Kennison & Chan-Tin, 2021; Yilmaz & Cetin, 2023; Cusack & Adedokun, 2018).

Neuroticism is characterized by emotional instability, anxiety, and sensitivity to stress (Credé et al., 2012; Luo et al., 2023; Matulessy & Humaira, 2016). People with low Neuroticism tend to manage stress better than those with high Neuroticism (Credé et al., 2012; Soutter et al., 2020). High Neuroticism is associated with greater caution and adherence to security protocols; however, emotional reactivity can make individuals more susceptible to manipulation and Social Engineering attacks (Papatsaroucha et al., 2021; Cho et al., 2016).

The five core traits provide a comprehensive map of human personality, capturing a vast range of behavioral, emotional, and cognitive tendencies. While each trait is defined independently and measured on separate scales, they do not operate in isolation. In practice, traits interact and reinforce one another, especially within social and environmental contexts. For instance, Extraversion and Agreeableness influence how individuals engage with others, and specific behavioral expressions may reflect the combined impact of multiple traits (Luo et al., 2023; Matulessy & Humaira, 2016). Extraversion is characterized by sociability, assertiveness, spontaneity, energy level, dominance, and confidence, and overlaps with high Agreeableness (Luo et al., 2023; Matulessy & Humaira, 2016). Those who are highly Extroverted often thrive in social environments and are described as very outgoing (Ji & Esqueda, 2022; Matulessy & Humaira, 2016). Agreeableness relates to interpersonal tendencies such as kindness, empathy, and cooperation, fostering a nurturing and supportive atmosphere while maintaining relationships (Luo et al., 2023; Matulessy & Humaira, 2016). High Agreeableness is associated with harmonious relationships and altruistic behavior, and, similar to Extroversion, also thrives in social environments (Matulessy & Humaira, 2016; Soutter et al., 2020).

Each trait has its own indicators and benchmarks that serve as metrics for individual characteristics, helping determine where each person lies on the trait spectrum (Matulessy & Humaira, 2016). For example, Extraversion evaluates sociability, assertiveness, outgoingness, activity levels, energy, and positive emotions (Matulessy & Humaira, 2016). Those who score high in sociability are typically engaging and friendly, whereas lower scores indicate shyness and reserve (Matulessy & Humaira, 2016). Research highlights the impact of various external variables on personality traits (Mamadov, 2022). Internal and external influences can affect behaviors and personality traits (Carvalho, Pianowski, & Gonçalves, 2020; Soutter et al., 2020).

Genetic background and environmental experiences shape an individual's personality traits and position within the Big Five model (Matulessy & Humaira, 2016). Although personality traits are considered relatively stable throughout one's life, studies indicate that people may react differently to similar situations due to distinct external factors (Fagade et al., 2017). This is crucial in understanding the choices made by threat actors during cyber-attacks.

Given the complexities of personality and trait naming, understanding these interactions is vital in practical areas like cybersecurity, where personality-driven decisions can have substantial effects. Each individual's traits and their interactions shape distinct personality typologies (Garcia & Moraga, 2017).

Big Five and Cybersecurity

The Big Five framework has become widely accepted and empirically validated as a foundational model for studying personality, applicable across domains, including cybersecurity (Ashton, 2022; Goldberg, 1990). While the model has some criticisms, including its limited attention to deeper constructs such as identity formation and motivations, it remains a foundational tool for personality assessment (Dyce, 1997). In cybersecurity research, the Big Five offers a valuable lens to examine how personality traits may influence one's propensity to engage in hacking and cyber intrusion behaviors (Albladi & George, 2017; Bashir et al., 2017; Coutinho et al., 2013; Gratian et al., 2018; Russell et al., 2017).

The Big Five has been extensively studied and validated across various domains of psychology and is often applied in cybersecurity research (Credé et al., 2012; Matulessy & Humaira, 2016; Shappie et al., 2019). The evolution of the Big Five and its widespread use across diverse populations demonstrates that it is a well-grounded framework suitable for

examining personality differences in various domains, including cybersecurity (Credé et al., 2012; John et al., 2008; Matulessy & Humaira, 2016; Shappie et al., 2019).

The broad adoption and extensive use of the Big Five Inventory have facilitated understanding of personality across various contexts (Ashton, 2022). Specifically, the Big Five correlates with tendencies toward risk-taking and social manipulation, consistent with hacking behavior (Ashton, 2022). These insights support the model's validity for studying the hacker population. A summary of each Big Five trait, along with corresponding hacker behaviors and supporting studies, is provided in Table 2.

Table 2.

Big Five Traits and Hacking Behavior

Big Five Trait	Key Characteristics	Hacker Behavior Associations	Notable Studies
Openness	Creative, curious, open to new experiences, abstract thinker	Linked to innovative black hat tactics; associated with abstract problem-solving and tech curiosity	Cho et al. (2016); Matulessy & Humaira (2016); Shappie et al. (2019); Yilmaz & Cetin (2023)
Conscientiousness	Disciplined, organized, responsible, goal-oriented	Higher levels reduce risky behavior; lower levels linked to disregard for security best practices	Fagade et al. (2017); Frauenstein (2021); Van de Weijer & Leukfeldt (2017); Zell & Lesick (2022);
Extraversion	Sociable, energetic, assertive, talkative	Some hackers display Extraversion; may reflect boldness or confidence in social manipulation	Bashir et al. (2017); Frauenstein (2021); Gerber et al. (2017); Russell et al. (2017)
Agreeableness	Kind, cooperative, empathetic, trusting	Low levels associated with suspicion and malicious behavior; high levels tied to cooperation	Cusack & Adedokun (2018); Kennison & Chan-Tin (2021); Yilmaz & Cetin (2023)
Neuroticism	Emotionally reactive, anxious, prone to stress	May influence stress response and caution; reactivity could increase or decrease attack engagement	Cho et al. (2016); Frauenstein (2021); Papatsaroucha et al. (2021)

Personality traits can serve as indicators of whether individuals are likely to engage in cyber-attacks or risky cyber behavior (Fagade et al., 2017; Kennison et al., 2021; Maimon et al., 2017; Papatsaroucha et al., 2021). For instance, research has found that black hat hackers, or those engaging in malicious hacking activities, tend to exhibit higher levels of Openness than

white hat hackers, or ethical hackers (Matulessy & Humaira, 2016). High levels of Openness among black hats may be linked to their curiosity and desire to hack, as well as to their creative technical abilities when working on complex issues, such as exploiting vulnerabilities or developing new technologies (Matulessy & Humaira, 2016). The creative aspect of Openness allows these individuals to hack innovatively, often leading to the discovery of novel methods for system intrusion. Openness is associated with complex and original thought patterns, which can facilitate adaptability with the ever-changing technical landscapes (Shappie et al., 2019). Hackers with high Openness may demonstrate greater abstract thinking and pattern recognition, essential for identifying weaknesses and vulnerabilities in cybersecurity systems (Matulessy & Humaira, 2016; Shappie et al., 2019). Openness is also associated with one's receptiveness to new cyber experiences, curiosity, and desire to continually learn and experiment with technology advancements (Matulessy & Humaira, 2016; Shappie et al., 2019).

Understanding the early signs of risky cyber behavior and malicious intent is essential for proactive, preventive measures against cyber-attacks (Fagade et al., 2017). Several studies have indicated that older adult men engage in riskier cybersecurity behaviors and exhibit higher Conscientiousness on the Big Five Inventory (Alohali et al., 2018; Kennison & Chan-Tin, 2021; McCormac et al., 2016; Russell et al., 2017; Shappie et al., 2020). Gerber, Gerber, and Hernando (2017) found that individuals with higher levels of Extraversion and lower levels of Agreeableness are more likely to use privacy protection strategies on their social networking sites, revealing less personal information than their introverted counterparts. In contrast, those who are more likely to adhere to cybersecurity best practices tend to score higher in Agreeableness and Neuroticism but are also more susceptible to victimization, being deceived by Social Engineering tactics, such as phishing (Cho et al., 2016; Cusack & Adedokun, 2018;

Kennison & Chan-Tin, 2021; McCormac et al., 2016; Papatsaroucha et al., 2021; Russell et al., 2017; Yilmaz & Cetin, 2023). Studies show that individuals lower in Agreeableness are more likely to adopt less cooperative online interaction strategies and remain suspicious of others (Kennison & Chan-Tin, 2021).

Ransomware victimization has been linked to personality traits such as Agreeableness and Openness (Yilmaz & Cetin, 2023), suggesting that those who are highly trusting, curious, or open to new experiences may be more susceptible to social manipulation or coercive attack vectors. This finding is particularly relevant given the prevalence of ransomware and the deliberate exploitation of perceived psychological vulnerabilities in early-stage attack strategies for initial access (Yilmaz & Cetin, 2023).

The relationship between personality and cybersecurity behavior becomes more complex when considering the broader literature. While Openness has been associated with greater susceptibility to phishing and exploratory risk-taking (Cho, Cam & Oltramai, 2016), other studies have linked Agreeableness not only to victim vulnerability but also to threat actor behaviors, particularly in contexts involving the exploitation of trust and Social Engineering (Fagade et al., 2017). These seemingly contradictory findings underscore a key limitation in existing research: personality traits do not map cleanly onto fixed roles of "victim" or "attacker."

The expression of personality appears to depend on situational context, opportunity, and intent. This ambiguity underscores the need to move beyond trait-based labels and toward examining how personality influences decision-making during cyber intrusions, regardless of whether those traits manifest in victimization or adversarial behavior.

Previous research has also explored the role of personality in cybersecurity personnel to improve intervention methods and customize training based on individual behavioral and

cognitive traits (Kennison & Chan-Tin, 2020; Russell et al., 2017). A considerable portion of the literature focuses on victims' personality traits to determine who is more susceptible to cyber-attacks (Budimar et al., 2021; Pratama et al., 2022; Van de Weijer & Leukfeldt, 2017). In this area of research, the Big Five Framework has been widely used to understand human vulnerability to cyber threats and to identify associations with a higher risk of victimization (Gerber, Gerber, & Hernando, 2017; Papatsaroucha et al., 2021).

Both qualitative and quantitative studies have examined how personality relates to susceptibility to Social Engineering, moral decision-making, and manipulative or exploratory behaviors (Budimir et al., 2021; Cho, Cam, & Oltramai, 2016; Cusack & Adedokun, 2018; Kennison et al., 2021; Kennison & Chan-Tin, 2021; Troisi et al., 2020). However, while this literature provides valuable insight into victim risk and defensive awareness, it offers a limited explanation of how these same personality traits shape the active decision-making processes of individuals engaging in cyber intrusion behaviors. This distinction highlights the need for research that examines personality not only in terms of vulnerability or prevention but also in terms of how individuals reason through, justify, and execute intrusion strategies.

Additionally, research has contributed to an understanding of how personalities can influence the risk of using technical know-how to gain a competitive advantage or leak insider information (Budimar et al., 2021; Fagade et al., 2017; Pratama et al., 2022; Russell et al., 2017; Sailio et al., 2020). Research has found that those who seek immediate gratification and lack self-control may be prone to future malicious or risky cyber activities (Van de Weijer & Leukfeldt, 2017). The overlap of Agreeableness, Conscientiousness, and self-control has been shown to correlate with the prediction of malicious behaviors (Van de Weijer & Leukfeldt, 2017).

Threat actors are increasingly leveraging social networking sites as a first line of attack, as these platforms provide a rich source of information about targets and enable indirect attacks that can facilitate access to desired corporate or governmental technical networks (Albladi & Weir, 2018). This requires understanding the personality traits of individuals at higher risk of victimization who follow low self-protective practices and engage in risky cyber behaviors, as these behaviors may serve as entry points for threat actors (Frauenstein, 2021). Behaviors such as using weak passwords or oversharing personal information on social networking sites can indicate who is more likely to be targeted within an organization (Frauenstein, 2021). A 2021 study collected data from over 200 graduate students to evaluate susceptibility to phishing on social networking sites based on personality traits (Frauenstein, 2021). The researchers concluded that individuals with extroverted and agreeable personalities were more likely to fall victim to phishing attempts, while conscientious individuals were less likely to do so (Frauenstein, 2021).

Additionally, users who scored higher on the test's self-efficacy components were less likely to engage in phishing behavior. In contrast, those influenced by social norms were at increased risk of phishing. The researchers also found that extroversion, combined with low self-efficacy, narcissistic charisma, and reduced empathy (Paulhus & Williams, 2002), may be associated with a heightened risk of cyber threat behaviors. These findings align with those of Van der Schyff et al. (2020), indicating that various antisocial personality traits, including a lack of empathy combined with extroversion (an otherwise social trait), may predict susceptibility to cyber-attacks and victimization.

The Big Five is a valuable tool for understanding an individual's core traits and assessing the potential inclination toward hacking behavior (Albladi & George, 2017; Bashir et al., 2017;

Coutinho et al., 2013; Gratian et al., 2018; Russell et al., 2017). Prior research indicates that individuals who engage in hacking behavior tend to be highly extroverted, which contradicts the typical stereotype of hackers. However, not all extraverted individuals engage in hacking behavior (Albladi & George, 2017; Bashir et al., 2017; Coutinho et al., 2013; Gratian et al., 2018; Russell et al., 2017). The Big Five is effective for examining both positive and neutral personality traits, which is particularly important when considering hacker typology. Despite its widespread adoption, some critiques have been raised regarding the scope of the Big Five model. Some researchers argue that while it effectively categorizes surface-level traits, it does not address deeper constructs such as motives, identity formation, or darker aspects, including underlying malicious and harmful behaviors (Amo et al., 2023; 2017; Dyce, 1997; Gratian et al., 2018; Russell et al.). Nonetheless, the Big Five remains one of the most extensively validated frameworks for personality assessment; however, it highlights the need for additional inventories, such as the Dark Triad, to understand the dark side of personality typology (Amo et al., 2023; Gratian et al., 2018; Russell et al., 2017).

In summary, the Big Five model offers a structured approach to understanding personality through five key dimensions that capture diverse aspects of human behavior. Its reliability across different populations and contexts has solidified its position as a cornerstone in psychological research (Ashton, 2022; Goldberg, 1990).

The Dark Triad

The Dark Triad framework (Paulhus & Williams, 2002) is the second framework chosen to understand threat actors' personalities and tactical cyber-attack decisions. The Dark Triad explains the character traits and implications of three specific malevolent personality traits - Narcissism, Machiavellianism, and Psychopathy. These traits align with the stereotypical societal

ideology of a threat actor (Matulessy & Humaira, 2016). Originally introduced during the early 2000s (Paulhus & Williams, 2002), the Dark Triad explains the cohesion of these three personality traits, characterized by manipulative behaviors, a lack of empathy, emotional coldness, aggressiveness, and a focus on self-interest (Maasberg, Warren, & Beebe, 2015). The three traits are "overlapping, but distinct" and represent attributes harmful to society (Haz et al., 2022). Based on psychological research, the framework has evolved to explain various aspects of these characteristics and their implications within social and organizational contexts (Furnham et al., 2013; Jonason et al., 2021; Jones & Paulhus, 2014; Paulhus & Williams, 2002).

The Dark Triad is often viewed as a valuable framework for understanding the personalities of individuals who engage in hacking behaviors, building on insights from the Big Five (Amo et al., 2023; Gaia et al., 2022). It helps clarify the influential precursors to unethical and deviant behaviors (Amo et al., 2023; Gaia et al., 2022). The three traits emphasized by the Dark Triad are unique in that they focus on specific malevolent personality traits (Hudson, 2022; Kaufman et al., 2019; Maasberg et al., 2020; Muris et al., 2017; Paulhus & Williams, 2002). A summary of each Dark Triad trait, its key characteristics, and its association with hacking behavior is presented in Table 3.

Table 3.

Dark Triad Traits and Hacking Behavior

Dark Triad Trait	Key Characteristics	Hacker Behavior Associations	Notable Studies
Narcissism	Excessive self-interest, grandiosity, egocentrism, need for recognition, lacks consideration for others.	Motivated by ego and recognition; may take credit for attacks using pseudonyms; may withhold security info in training.	Ahmed & Islam (2022); Amo et al. (2023); Paulhus & Williams (2002); Sanders (2021)
Machiavellianism	Manipulative, strategic, exploitative, pragmatic, uses others to achieve goals, morally disengaged.	Strategically exploits human and system vulnerabilities; plans attacks to maximize gain and minimize detection.	Amo et al. (2023); Gaia et al. (2020); Gaia et al. (2022); Maasberg et al. (2020); Paulhus & Williams (2002)
Psychopathy	Impulsive, thrill-seeking, emotionally cold, low empathy, antisocial behavior, reckless with no planning.	Engages in high-risk attacks without concern for consequences; impulsivity leads to immediate gratification from attacks.	Amo et al. (2023); De Paoli & Johnstone (2023); Jones et al. (2021); Paulhus & Williams (2002)

Narcissism, the first personality trait in the Dark Triad, is characterized by excessive interest and a focus on oneself at the expense of others, along with a grandiose sense of self (Haz et al., 2022; Maasberg, Warren, & Beebe, 2015). In the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-V), Narcissism is classified as a personality disorder, and individuals clinically display an exaggerated sense of self, heightened fantasies of success, and highly disagreeable, aggressive behavior (Furnham et al., 2013; Haz et al., 2022; Jonason et al., 2021; Maasberg, Warren, & Beebe, 2015; Paulhus & Williams, 2002). Narcissists are characterized by a grandiose sense of self and an overconfident nature, and they do not believe strategic planning is required (Jones, 2022; Kaufman et al., 2019; Maasberg et al., 2020; Wang et

al., 2022). They are highly self-centered, driven by their ego, and believe the world owes them something (Jones, 2022; Maasberg et al., 2020). Narcissists are not necessarily seeking to harm others. Instead, they are focused on themselves and their own goals and do not consider how their choices may impact others (Maasberg et al., 2020).

Machiavellianism is a personality characteristic characterized by pragmatism and a cunning nature and is understood to be exemplified through manipulation, exploitation of others, and strategic thinking to achieve personal goals (Haz et al., 2022; Maasberg, Warren, & Beebe, 2015; Maimon et al., 2017; Paulhus & Williams, 2002).

Psychopathy is a term used to describe individuals with high impulsivity, low empathy, and anxiety, often displaying criminal tendencies, extreme thrill-seeking behaviors, and severe antisocial characteristics (Haz et al., 2022; Maasberg, Warren, & Beebe, 2015; Paulhus & Williams, 2002). Psychopathy is considered a subclinical domain in which individuals have learned to function within society without severe punishment, such as institutionalization (Jones et al., 2021). Those high in Psychopathy are deceptive, antisocial, and impulsive (Jones et al., 2021; Jones, 2022). These individuals tend to engage in reckless situations, often with little to no planning (Jones et al., 2021; Jones, 2022). The thrill drives Psychopaths and leads to a lack of concern about being caught, due to their low levels of anxiety and callousness (Kaufman et al., 2019; Maasberg et al., 2020; Wang et al., 2022). Due to their impulsive nature, they often accept a small, short-term gain, even when the risk is high (Jones, 2022).

The nuance of each trait is distinct; however, all three are socially malicious and detrimental to society (Haz et al., 2022; Kaufman et al., 2019; Maasberg et al., 2020; Miao et al., 2023; Vedel & Thomsen, 2017). Despite the independent and unique nature of the traits, there is distinct overlap, such as highly deceptive behaviors, lack of concern over potential negative

impacts on others, being manipulative, and focusing on behaviors that meet their self-interests (Егорова, 2019; Hudson, 2022; Kaufman et al., 2019; Wang et al., 2022). The three traits share a malicious, dark nature, in which individuals disregard the potential impact of their behaviors on others for self-serving gratification (Johnson et al., 2019; Maasberg et al., 2020; Wang et al., 2022). As noted by Yin et al. (2023), the Dark Triad traits are characterized by self-interest, maliciousness, manipulation, and exploitation.

Motivators of bad behavior manifest differently across the three dark traits (Maasberg et al., 2020). Machiavellians misbehave for personal gain (Maasberg et al., 2020). They are often seen as cynical and strategic in their actions, thoughtfully planning before engaging in deviant behaviors to maximize benefits and minimize risks (Jones, 2022; Kaufman et al., 2019; Maasberg et al., 2020; Wang et al., 2022). Machiavellians are characterized by calculated, manipulative thinking, a focus on how they can influence others to achieve objectives, and concern for adverse effects on others (Kaufman et al., 2019; Maasberg et al., 2020; Wang et al., 2022).

Like the Big Five, the Dark Triad theory assumes that Narcissism, Machiavellianism, and Psychopathy form a continuum, with some individuals exhibiting higher levels of these traits than others. The traits are not mutually exclusive, as they are generally viewed on a spectrum, allowing for varying degrees of each trait (Johnson et al., 2019). An individual does not necessarily need to possess all three dark traits, though this is possible (Gaia et al., 2021; Gaia et al., 2020; Gaia et al., 2022; Johnson et al., 2019). They may exhibit only one trait or varying degrees of multiple traits (Gaia et al., 2021; Gaia et al., 2020; Gaia et al., 2022; Johnson et al., 2019).

The Dark Triad also indicates that these traits are interconnected, suggesting that their behavioral aspects are (Paulhus & Williams, 2002). Some individuals exhibit multiple traits simultaneously, while others show only one. The presence of these personality traits, particularly in combination, is associated with negative social ramifications, such as strained social and organizational relationships, due to manipulative behaviors that often prioritize self-interest over others' interests and demonstrate a lack of empathy (Furnham et al., 2013; Jonason et al., 2021; Jones & Paulhus, 2014; Paulhus & Williams, 2002). Furthermore, the Dark Triad posits that individuals who display all three personality traits simultaneously pose a greater risk to society due to the social dangers inherent in these characteristics and their compounded effects (Paulhus & Williams, 2002).

The intent to engage in cyber risk-taking can be positively associated with displaying narcissistic characteristics, which may lead to an understanding that cyber threat actors also exhibit this characteristic (Ahmed & Islam, 2022). However, further research is needed to validate this assumption (Harms et al., 2022). Narcissism, characterized by the need for recognition (Amo et al., 2023), may not necessarily correlate with malicious behaviors since many cyber-intrusive behaviors are intended to be carried out covertly without gaining attribution (Gaia et al., 2020). However, those who display narcissistic characteristics display traits categorized by self-interest, suggesting threat actor behaviors, which threat actors, traditionally believed to be motivated by personal gain, may be predicted by narcissistic traits (Ahmed & Islam, 2022). Furthermore, Narcissism is marked by egocentric behavior, such as taking credit for attacks, which can manifest through the use of pseudonyms and alternate personas to seek validation and recognition (Sanders, 2021).

Machiavellians may strategically exploit vulnerabilities in the human element and weaknesses inherent in corporate technological and security systems (Gaia et al., 2020; Sanders, 2021). A notable example is the Wells Fargo scandal, in which many employees took advantage of customers for personal financial gain by opening fake checking accounts in their names, resulting in excessive and fraudulent fees (Office of Public Affairs, 2020). Although the psychological origins of these employees' behaviors are unknown or unproven, this case illustrates the potential outcomes of Machiavellian behavior (Amo et al., 2023). Despite these behaviors, the extent or presence of Machiavellianism among malicious threat actors remains unknown (Harms et al., 2022).

In the context of current knowledge regarding Psychopathy among threat actors, a synthesis of research reveals that Psychopathy may manifest as a lack of empathy and an increased propensity for risk-taking behavior (Amo et al., 2023; De Paoli & Johnstone, 2023; Gaia et al., 2020; Paulhus & Williams, 2002; Sanders, 2021). However, the extent of Psychopathy among threat actors remains unclear and underexplored (Harms et al., 2022), emphasizing the need for more research. Nevertheless, a lack of empathy may drive individuals with psychopathic traits to engage in risky cyber behavior, compromising the security of systems, without regard for the consequences of their actions on colleagues, organizations, and other clients and consumers (Amo et al., 2023; De Paoli & Johnstone, 2023; Gaia et al., 2020; Paulhus & Williams, 2002; Sanders, 2021). When coupled with one or two other characteristics of the Dark Triad, such a tendency can create an exceptionally threatening personality profile due to the combined indifference toward others and self-serving, deceptive behavior (Paulhus & Williams, 2002; Sanders, 2021). In such instances, there would be little motivation for a threat actor to refrain from a cyber-attack.

The impact of the Dark Triad traits among threat actors in cybersecurity contexts is challenging, if not impossible, to quantify. However, researchers suggest that these traits pose a significantly greater, multidimensional threat to organizations than system glitches or technical errors (Amo et al., 2023; De Paoli & Johnstone, 2023; Gaia et al., 2020). Since culture is considered the foundation from which technically efficient security systems develop (Petry, 2011), the presence of malicious personality traits, such as those associated with the Dark Triad, can be hypothesized to pose substantial financial, cultural, and security risks to the overall threat landscape (Amo et al., 2023; De Paoli & Johnstone, 2023; Gaia et al., 2020).

Some existing research explores the intersection of Dark Triad personality traits and their influence on victim outcomes, showing that narcissistically driven attacks increase the likelihood of victimization, while Machiavellianism does not (Amo et al., 2023). Moreover, Hussain et al. (2021) found that the presence of all three Dark Triad personality traits simultaneously within an individual is more positively and significantly associated with problematic Internet usage, including hacking behavior, pornography use, violence, exploitation, and other unlawful or malicious activities. Hussain et al.'s (2021) findings, alongside Amo et al.'s (2023) research, suggest that exhibiting narcissism, or all three facets of the Dark Triad in combination, may have more harmful implications than Machiavellianism alone. Additionally, Machiavellianism is positively associated with moral disengagement. At the same time, Machiavellianism and psychopathy in combination are shown to be linked to euphemistic language and an increased threat of social harm (Maftei et al., 2022), further supporting the idea that when these threats exist together, the repercussions can be more devastating, especially in the context of cybersecurity (Bada & Nurse, 2021; Bada & Nurse, 2023; Foster & Cross, 2024; Jones, 2022; Laakasuo et al., 2020).

Despite researchers emphasizing the need to recognize these character traits as indicators of threat and risk in cybersecurity, Hess (2022) underscores the importance of educating organizations, leaders, and employees to identify rather than mislabel or misdiagnose potential personality traits. For instance, some antisocial behaviors may indicate other conditions, such as autism (Wagner et al., 2022), but are often mistaken for traits associated with the Dark Triad (Paulhus & Williams, 2002; Yoon et al., 2021). Moreover, some researchers suggest that higher rates of autism may characterize individuals as threat actors rather than as people engaged in more socially normative roles (Wagner et al., 2022), thus further highlighting the need for critical and accurate screening of individuals instead of mislabeling personality traits or character conditions.

In the cybersecurity culture, there are self-reported white and black hat hackers. These individuals utilize their technical intrusion skills for either good (white hat) or bad (black hat) purposes (Black, 2022). White hat hackers are security professionals who make positive contributions to society or organizations through their hacking abilities, including ethical hackers (Abbott, 2019; Black, 2022). Although those who self-identify as white hats are generally recognized for making beneficial contributions to organizations or communities, personality traits associated with the Dark Triad may inherently emerge within this group (Abbott, 2019; Black, 2022). For example, regarding security and awareness training, white hat security professionals are typically seen as responsible for delivering more transparent, comprehensive, up-to-date, and robust awareness training. However, Dark Triad personality traits may lead some individuals to withhold information for personal gain or to use deceptive communication strategies, potentially resulting in compromised training where information is withheld,

misconstrued, or presented in a manner that serves the self-interests of narcissistic, psychopathic, and/or Machiavellian individuals (Abbott, 2019; Padayachee, 2022).

Black hat hackers are individuals who exploit their technical skills and authority to maliciously threaten the well-being of organizations, communities, or others through intentional cyber-attacks or breaches (Abbott, 2019; Black, 2022). The misuse of skills, power, or privileges can involve mishandling cybersecurity knowledge, elevated privileges, passwords, or proprietary information, as well as exploiting, manipulating, and deceiving others to carry out hacks or breaches for personal gain (Abbott, 2019; Black, 2022). Due to the intentional malevolence associated with Dark Triad personality traits, these traits are theorized to be more prevalent in black-hat communities than in white-hat ones (Abbott, 2019; Black, 2022; Paulhus & Williams, 2002). However, further research is needed to validate this presumption (Harms et al., 2022).

The Dark Triad traits may manifest through malicious practices, deceptive use of power, and self-interested, risk-taking behaviors (Abbott, 2019; Black, 2022; Paulhus & Williams, 2002). For example, typical psychological and physiological responses to crime or harm may include remorse or empathy; however, individuals with Dark Triad personality traits often show a lack of remorse or understanding regarding their harmful actions (Silic & Lowry, 2019). Furthermore, threat actors may use dissociation as a coping mechanism to manage these behaviors, implying the presence of dissociative personality traits as well (Silic & Lowry, 2019).

Several studies suggest that elements of the Dark Triad, such as deception and manipulative behaviors, enable many threat actors to navigate their daily lives undetected, leading to even greater risks due to their inconspicuous and unsuspecting nature (Filiol et al., 2021). For example, while many people may assume that threat actors are antisocial and outright malicious (Goerzen, 2021), many demonstrate extroverted behaviors filled with charm and

charisma, alongside hidden malicious intent and deception, traits associated with overt Narcissism (Goerzen, 2021; Okpa et al., 2022; Paulhus & Williams, 2002). Instances of these traits among black hats, which can pose significant threats to the public, community, and institutions, include impersonators and scammers. For example, scammers impersonating representatives of wireless cellular service companies or Best Buy's Geek Squad may intercept customer service calls. Through a deceptive process of guiding unsuspecting clients under the guise of customer service, they can collect individuals' PII and financial data, which can serve as an entry point for further attacks via unauthorized credential access and fraudulent accounts (Bates, 2023; Filiol et al., 2021).

Another aspect frequently discussed in the reviewed literature on the Dark Triad is the intersection of modern pop culture and the cybersecurity landscape (Shires, 2019). In contemporary pop culture, a genre of hackers known as red hat and grey hat hackers is emerging, referring to independent vigilantes who aim to address vulnerabilities and prevent cyber-attacks, often working in professional IT fields (Filiol et al., 2021; Matulessy & Humaira, 2016). Some researchers suggest that red hat hackers may be less likely to exhibit the Dark Triad personality traits, as they operate independently and are motivated by vigilante actions and recognition (Filiol et al., 2021; Okpa et al., 2022). The complexities surrounding the motivations behind the hacking behaviors of white, black, and grey hat hackers may relate to the Dark Triad personality traits, but further research is needed to confirm this assumption (Harms et al., 2022; Shires, 2019).

The published empirical literature reviewed in this section synthesizes recent evidence and discussion on the intersection of the Dark Triad personality traits and cyber-threats, providing a basis for contextualizing the proposed study's problem and the gap in research

supporting its need. As described, the existing literature linking cybersecurity actors to Dark Triad personality traits is scarce yet emerging.

Differentiation Between the Big Five and Dark Triad

It is essential to understand the differentiation between the Big Five and the Dark Triad. Dark traits are considered maladaptive and pervasive, falling outside the purview of the Big Five (Hudson, 2022; Jonason et al., 2020; Lee et al., 2013; Maasberg et al., 2020; Neumann et al., 2021). The Dark Triad complements the Big Five by accounting for dark traits that do not fit into the standard Big Five representation, such as cynical worldview, absence of morality, manipulative and deceptive tendencies, grandiosity, and emotional callousness (Lee et al., 2013; Hudson, 2022; Jonason et al., 2020; Jones, 2022). While there are overlaps and commonalities between the two scales, such as levels of Agreeableness, the traits of both scales have distinct nuances (Haz et al., 2022; Maasberg et al., 2020; Neumann et al., 2021; Vedel & Thomsen, 2017; Wang et al., 2022).

In criminology, the Dark Triad is considered a reliable predictor of whether an individual will engage in illegal or deviant behavior over their lifetime. In contrast, the Big Five offers insights into normative behaviors, such as occupational decision-making and well-being (Hudson, 2022; Neumann et al., 2021). It is essential to note that although the Dark Triad encompasses behaviors that go beyond the scope of the Big Five, individuals exhibiting Dark Triad traits still possess Big Five traits as part of their personality (Furnham et al., 2013; Grigoras & Wille, 2017; Hudson, 2022).

The distinction between the two frameworks lies in their conceptualization and focus. The Dark Triad encompasses traits that are malevolent, maladaptive, abnormal, and pervasive, whereas the Big Five represents five broad normative personality dimensions observable in all

individuals (Furnham et al., 2013; Garcia & Moraga, 2017; Jonason et al., 2021; Jones & Paulhus, 2014; Matulessy & Humaira, 2016; Maasberg et al., 2020; Mammadov, 2022; Miao et al., 2023; Paulhus & Williams, 2002). The Big Five is often viewed as reflecting positive, neutral, and socially desirable traits, while the Dark Triad captures the darker aspects of personality that lie outside the Big Five, such as manipulation or callousness (Busuioc & Butucescu, 2020; Grigoras & Wille, 2017; Musek & Grum, 2021). All individuals are considered to possess the Big Five traits, though to varying degrees; not everyone exhibits Dark Triad traits (Hudson, 2022; Muris et al., 2017). For this reason, the Dark Triad may provide significant insights into hacking propensity and the chosen TTPs (Jones et al., 2021).

At extreme levels, the Big Five traits can become maladaptive, but they are usually not dark or socially pervasive (Grigoras & Wille, 2017). For instance, someone might score low on Agreeableness (Grigoras & Wille, 2017). A low level of Agreeableness does not necessarily lead to dark or socially disruptive behaviors, although it is possible (Grigoras & Wille, 2017). When these traits become severe, they may overlap with the Dark Triad, resulting in abnormal behaviors that could harm society (Furnham et al., 2013; Grigoras & Wille, 2017; Paulhus, 2014).

Research indicates that personality tends to be relatively stable throughout a person's life and significantly influences the choices an individual makes (Allemand et al., 2010; Cobb-Clark & Schurer, 2011; Measelle et al., 2005; Rantanen et al., 2007). Notably, studies show that many people wish to change certain aspects of their Big Five personality traits in positive ways; however, this desire for change does not apply to those who display Dark Triad traits (Baranski et al., 2017; Hudson, 2022; Hudson et al., 2019; Hudson & Fraley, 2015; Hudson & Fraley, 2016; Miller et al., 2019; Quintus et al., 2017). It is often suggested that, if personality and

behavioral indicators linked to deviance and hacking are identified early enough, interventions can be implemented, guiding individuals away from malicious hacking towards more constructive uses of their talents for the benefit of society (Xu & Zhang, 2013).

The two personality constructs exist on a continuum in how traits are expressed, enabling individuals to manifest high or low levels of different characteristics. However, because dark traits are outside the Big Five framework, the two scales must remain separate to capture the maladaptive and criminal behaviors seen in society fully (Garcia & Moraga, 2017; Garcia et al., 2015; Hudson, 2022; Maasberg et al., 2020; Paulhus & Williams, 2002; Veselka et al., 2011). Although these models represent distinct personality traits, understanding their interactions is essential for understanding behavior and personality.

The Intersection of the Big Five and Dark Triad

Research shows that the two domains are not isomorphic, with each model containing specific attributes necessary to reflect an individual's unique personality (Jones et al., 2021; Neumann et al., 2021). While the Dark Triad is often considered a better predictor of malevolent behavior, the Big Five provides a foundation for understanding personality (Jones et al., 2021; Neumann et al., 2021). Using both scales together can help distinguish among different hacker types and forecast a hacker's potential path (Gaia et al., 2022; Jones et al., 2021). Although the models differ, they intersect, and understanding this relationship is essential for gaining deeper insights into how personality relates to hacking (Gaia et al., 2021; Gaia et al., 2020; Gaia et al., 2022).

The traits in both models are unique and relatively independent constructs (Garcia & Moraga, 2017). None of the characteristics operates in a vacuum; each trait represents a distinct aspect of one's personality (Garcia & Moraga, 2017). The Big Five is estimated to account for

18-39% of the variance in the behaviors exhibited within the Dark Triad (Garcia & Moraga, 2017; Paulhus et al., 2021). While this range can be seen as a moderate association, it illustrates the overlap between the two models (Garcia & Moraga, 2017; Paulhus et al., 2021). Given that the Big Five do not account for 60% or more of the variance in dark traits, the need to maintain separate scales to address the wide range of characteristics is highlighted (Furnham et al., 2013; Garcia & Moraga, 2017; Paulhus et al., 2021).

As noted, personality is a complex construct that requires dynamic, adaptive approaches to fully understand how traits are expressed (Garcia & Moraga, 2017; Paulhus et al., 2021). Although prior research has examined personality in linear terms, it is now recognized that such approaches are inadequate given the complexities and nuances of each trait (Garcia & Moraga, 2017). The simultaneous display of multiple dark traits may lead to varied expressions of malevolent characteristics (Garcia & Moraga, 2017). For example, individuals with both psychopathy and narcissism may show higher levels of Extraversion than those who possess only one of these dark traits (Garcia & Moraga, 2017).

Trait Activation Theory (TAT) can support the dynamic understanding of individual differences and how and why certain traits are expressed (Jones & Mueller, 2021; Jones et al., 2021). TAT suggests that personality traits influence behavior in response to situations that are solid or weak (Jones & Mueller, 2021; Jones et al., 2021; Tamraker et al., 2016). For example, one could be high on the Machiavellianism scale. When they perceive an opportunity to exploit, their specific trait pattern may be triggered, leading them to engage in hacking behaviors (Jones & Mueller, 2021; Jones et al., 2021). The situational demands activate specific traits within an individual, which can predict whether one engages in an attack and potentially which TTPs they select (Jones & Mueller, 2021; Jones et al., 2021; Tamraker et al., 2016). Complicating the

understanding of how various traits are activated is the level of specific qualities one possesses, as the degree of each trait can influence perceptions of opportunities and willingness to engage in certain behaviors (Garcia & Moraga, 2017).

A major intersection between the Big Five and the Dark Triad is the level of Agreeableness (Furnham et al., 2013; Garcia et al., 2015; Garcia & Moraga, 2017; Hudson, 2022; Muris, 2017; O'Boyle et al., 2015; Paulhus & Williams, 2002; Paulhus et al., 2021). Agreeableness is characterized by trust, compliance, and tenderness and is positively associated with interpersonal relationships (Costa, McCrae & Dye, 1991; Muris, 2017; Paulhus et al., 2021). Agreeableness can become malevolent when one has a strong tendency to disagree with others, often leading to negative interpersonal relationships (Costa, McCrae & Dye, 1991; Muris, 2017; Paulhus et al., 2021). Given the spectrum nature of traits, Agreeableness becomes maladaptive when a person displays intense low levels of Agreeableness towards others or situations, rejecting social norms or authority (Garcia et al., 2015; Garcia & Moraga, 2017; Hudson, 2022; Muris, 2017; Paulhus & Williams, 2002; Paulhus et al., 2021).

Interestingly, various combinations of dark traits have been found to contribute to specific levels of the Big Five traits that individuals may exhibit (Furnham et al., 2013; Garcia & Moraga, 2017; Paulhus & Williams, 2002). For instance, those who score high in both Psychopathy and Narcissism tend to exhibit higher levels of Extraversion and Openness, whereas individuals high in both Machiavellianism and Psychopathy display lower levels of Conscientiousness (Furnham et al., 2013; Garcia & Moraga, 2017; Paulhus & Williams, 2002). Regardless of the combination of dark traits, all individuals show heightened levels of Disagreeableness (Furnham et al., 2013; Garcia & Moraga, 2017; Paulhus & Williams, 2002).

Another thematic relationship between the two models concerns how Agreeableness (or lack thereof) is expressed through negative psychosocial behaviors, including hacking, cyberbullying, disciplinary choices, workplace deviance, and attitudes toward cheating (Čopková & Christenková, 2021; Ellen et al., 2021; Geel et al., 2017; Jonason et al., 2011; Jones, 2022; Krick et al., 2016; Lee, 2019; Muris et al., 2017; Nicholls et al., 2019). Individuals low in Agreeableness tend to be antagonistic, aggressive, demanding, shrewd, intolerant, and uncooperative, and they show a lack of empathy toward others (Furnham et al., 2013). They often seek revenge and struggle to maintain positive relationships (Bajwa & Khalid, 2015). In the workplace, these individuals are more likely to resist organizational norms, resulting in unethical behavior, conflicts, disruptions, mistreatment of colleagues, a lack of professional commitment, and overall defiant and deviant actions (Ellen et al., 2021; Farhadi et al., 2012; Kaufmann et al., 2021).

Leveraging both The Big Five and Dark Triad scales can provide a comprehensive profile of individuals who engage in hacking, as each scale reveals distinct personality traits that shape one's personality profile and behavior patterns (Gaia et al., 2020; Gaia et al., 2022; Garcia & Moraga, 2017; Maasberg et al., 2020; Paulhus & Williams, 2002; Veselka et al., 2011). To fully understand an individual's unique personality and create effective threat profiles, both models should be employed together (Gaia et al., 2020; Gaia et al., 2022; Garcia & Moraga, 2017; Maasberg et al., 2020; Paulhus & Williams, 2002; Veselka et al., 2011).

The Dark Triad significantly influences unethical behavior and helps predict intent and sentiments related to hacking in general (Gaia et al., 2022; Amo et al., 2023; Pelster et al., 2021). The Big Five framework helps us understand behavioral patterns and decision-making based on an individual's unique traits (Garcia & Moraga, 2017). For instance, a person exhibiting Dark

Triad traits may exhibit different behaviors depending on their level of Extraversion in the Big Five (Garcia & Moraga, 2017). Although two individuals might score high on the Psychopathy scale, one may have higher Extraversion while the other has lower, resulting in distinct behavioral expressions (Garcia & Moraga, 2017).

It is essential to consider the hacker typology to understand how specific characteristics influence behaviors and intrusion decision-making. Research shows that Dark traits can predispose individuals to engage in practices or prioritize gain when the opportunity arises (Abbott, 2019; Padayachee, 2022; Thomas et al., 2018). This individual may have Narcissistic characteristics that, when the right conditions are present, allow them to utilize their skillset to hack for perceived altruistic or criminal purposes (Abbott, 2019; Padayachee, 2022).

Personality Models as a Predictor of Hacking Behavior

In the context of cybersecurity and hacking behaviors, understanding personality is a critical component of effective defense measures, threat anticipation, intrusion detection, and predicting hackers' TTPs (Ceccato et al., 2017; Ma, 2023). Although personality and behavior are complex constructs, specific traits and personality dimensions can be strong predictors of deviant and potentially illegal behaviors (Eronen & Romeijn, 2020; Naz et al., 2022; Schyns et al., 2019).

Research on the psychological aspects of cyber-attacks and the personality traits of threat actors is limited. One promising yet understudied research avenue concerning cybercrime prevention involves investigating psychopathy in relation to personality traits that may contribute to cybercrime (Haz et al., 2022; Jones et al., 2021; Rogoza & Cieciuch, 2019). According to Jones et al. (2021), analyzing personality traits outlined in the Big Five and the Dark Triad can strongly predict cyber-attacks that are deceptive and manipulative and compromise systems and

users. Furthermore, preliminary research indicates significant associations between specific personality traits and an elevated risk or propensity for cybercrime (Haz et al., 2022; Jones et al., 2021; Rogoza & Cieciuch, 2019; Selzer & Oelrich, 2021). This suggests that a deeper understanding of personality traits and their impact on cybercrime could lead to more effective interventions tailored for detection and prevention. For example, a study involving German computer science students used the theory of planned behavior to predict potential cybercrime and found a significant correlation between heightened Psychopathic and Machiavellian traits and intentions to engage in cybercrime and hacking (Selzer & Oelrich, 2021). These findings are particularly crucial for preventing insider attacks (Harms et al., 2022). Harms et al. (2022) stress that comprehending the relationship between Dark Triad and Big Five personality traits is vital for predicting and preventing insider threats, indicating that these traits are reliable indicators of workplace risks.

Researchers suggest that combinations of personality traits contribute to a higher rate of cyber-attacks and threats (Haz et al., 2022; Jones et al., 2021; Rogoza & Cieciuch, 2019; Selzer & Oelrich, 2021) because these traits undermine the essential elements of optimized security (Petry, 2011). However, Ock (2023) points out that one of the most overlooked aspects of ransomware is its psychological factors. Harms et al. (2022), Ock (2023), and Curtis et al. (2021) propose that the links between Dark Triad personality traits and cybersecurity warrant further exploration (Curtis et al., 2021).

Hackers need to stay stealthy in order to avoid detection by tools and defenders. It is known that those higher on the Psychopathy scale tend to act impulsively, ignoring the risk of noise (Jones et al., 2022). In contrast, individuals with higher Machiavellianism are more cautious, often engaging in planning and strategizing to evade detection (Jones, 2022). While

these traits are associated with illegal or criminal activities, their presence varies across individuals depending on their unique personality profiles (Curtis et al., 2021; Jones et al., 2021; Jones & Paulhus, 2017). This personality profile influences why some choose specific behaviors over others (Garcia & Moraga, 2017; Thomas et al., 2018). Understanding personality traits can shed light on why some individuals remain ethical hackers, while others become grey- or black-hat hackers (Garcia & Moraga, 2017; Thomas et al., 2018).

As noted, levels of Agreeableness influence the likelihood of someone engaging in hacking (Geel et al., 2017). Thrill-seeking, risk-taking, and resistance to authority are frequently identified as traits among individuals attracted to the hacking field, whether they engage in white-, grey-, or black-hat hacking (Gaia et al., 2020; Gaia et al., 2022). Individuals with Dark Triad characteristics often display antagonistic and risk-taking behaviors, aligning with the common perception of hackers (Ahmed & Islam, 2022; Rauthmann, 2011). Perceptions of being caught also affect the likelihood of engaging in hacking, which can be further understood through the Big Five personality traits (Gaia et al., 2022; Garcia & Moraga, 2017).

Personality traits can influence the choices and hacking methods one uses. Previous studies found that individuals who employed stealthy hacking techniques scored higher on the Machiavellianism scale (Jones et al., 2021). Conversely, those who adopted more aggressive tactics, such as brute force attacks, tended to rank higher in Narcissism and Psychopathy (Jones et al., 2021). This is significant as it indicates that the selected tactics often correlate with the individual's distinct personality traits (Jones et al., 2021; Jones et al., 2022). Research also illustrates that individuals within the Psychopathy spectrum typically demonstrate poor attention to detail, generally investing less time and effort into their cyber-attack tactics, and frequently failing to adapt their approaches even after unsuccessful attempts (Curtis et al., 2018; Jones,

2022). On the other hand, Machiavellian individuals are characterized by their strategic and cautious nature, dedicating more time to planning and adjusting their efforts, particularly after failed exploits (Curtis et al., 2018; Curtis et al., 2021; Jones, 2022). They are also noted for investing greater effort and focus into phishing attacks (Curtis et al., 2018; Jones, 2022).

It is often argued that dark traits can predict who will engage in cyber harassment, cyber aggression towards youth, insider threats, online dating abuse, and cyberbullying (Bhogal & Wallace, 2021; Gammon et al., 2011; Jones et al., 2021; Jones, 2022; Maasberg et al., 2015; Nocera & Dahlen, 2020; Yong-ping et al., 2018; Zhang et al., 2022; Zhang & Zhao, 2020). The Dark Triad is also a widely accepted predictor of in-person deviant and illegal behaviors, including but not limited to exploitative interpersonal behavior, aggression towards an intimate partner, petty theft and white-collar crime (Carton & Egan, 2017; Jones et al., 2021; Jones & Neria, 2018; Jones & Paulhus, 2017; Lingnau et al., 2017; Lyons & Jonason, 2015; Paulhus et al., 2021). It is also understood that dark traits are associated with positive attitudes towards various deviant behaviors, such as fraud and insider trading (Jones et al., 2022). However, research on specific personality traits inherent to hackers and how these traits inform TTP choices in cyber-attacks is limited (Harms et al., 2022; Jones et al., 2022; Ock, 2023). What is known from prior criminological research on dark traits is that it can be applied to hacking and intrusion behaviors, as the behaviors often parallel other settings and deviant behaviors (Back et al., 2010; Book et al., 2015; Christie & Gie, 2013; Curtis et al., 2018; Jones et al., 2021).

Research on the dark triad personality traits among those who conduct cyber-attacks shows that specific characteristics contribute to the TTPs chosen for their intrusion decisions (Curtis et al., 2018; Jones, 2022). However, more research is needed to understand this topic

better. Understanding individual trait makeup and differences can support proactive defenses and even enable early intervention and prevention (Kioskli & Polemi, 2020; Xu & Zhang, 2013).

Intrusion Behaviors

Understanding threat actors and the decisions they make during intrusions hinges on their goals, which may involve financial gain, causing interpersonal harm, or simply the thrill of demonstrating their ability to bypass security controls (Maimon et al., 2017; Romanosky & Boudreaux, 2021; Sailio et al., 2020). Over time, threat actors are becoming increasingly inventive in their hacking methods (Ma, 2021; Sailio et al., 2020). Unlike in the 1970s and 1980s, when social engineers would sift through garbage dumpsters for information, threat actors can now gather the necessary data to launch an attack remotely from almost anywhere (Olufunsho et al., 2022). Threat actors often develop new and innovative approaches as technology evolves, while also reviving or reimagining older techniques and technologies that may not be on defenders' radars to circumvent defenses (Sailio et al., 2020). Older threat technologies are being revived, broadening threat actors' arsenal well beyond traditional malware (Deepwatch, 2024).

Black hat hacking is considered unethical and often illegal, involving gaining unauthorized access to computer systems, accounts, applications, cloud networks, VPNs, or large organizational data lakes (Christen, Ranbaduge & Schnell, 2020; Romagna, 2019; Tanczer, 2019). These hacking practices can violate confidentiality, privacy, and compliance regulations, leading to costly and severe legal consequences (Klimburg-Witges & Wentland, 2021; Votipka et al., 2021). However, threat actors are frequently portrayed as "professional social engineers," carrying out attacks that challenge even the most skilled defenders to detect (Verizon, 2023), which can trigger significant negative emotions among victims (Budimir et al., 2021).

The increasing complexity of technologically advanced societies, including smart cities, smart medical systems, and critical infrastructure such as the power grid, has led to exponential growth in vulnerabilities and opportunities for exploitation (Ma, 2021; Sailio et al., 2020). As complexity rises, so does the attack surface (Sailio et al., 2020). Technical errors in system configuration, including misconfigurations and the fallibility of employees acting as system administrators, have created avenues for exploitation by threat actors (Verizon, 2022). Threat actors also understand that targeting individuals who are susceptible to cyber-attacks, such as phishing, and using stolen credentials to infiltrate a network is often an easy attack vector (Albladi & Weir, 2018; Verizon, 2022; Verizon, 2023). However, security practitioners report that information-stealing mechanisms are becoming increasingly sophisticated, targeting high-value targets and enabling threat actors to evade defenses more effectively (Deepwatch, 2024).

Intrusion methodology can exploit trust and relationships in the physical world to cause damage. While threat actors target vulnerabilities and technical deficiencies within a network, Social Engineering tactics help obtain information that may not be readily accessible (Cusack & Adedokun, 2018). For instance, organizations often use third parties, such as subcontractors, vendors, and auditors, to conduct business functions, creating a "trust" gap in the network where unintentional compromises can occur (Sailio et al., 2020). A lack of security controls for third-party service providers frequently creates a backdoor or opening for threat actors to exploit (Sailio et al., 2020). DTEX i3 (2023) found that from 2022 to 2023, the use of work-issued computers for unsanctioned or third-party work increased by 200%, and the use of non-business-approved applications rose by more than 50%. This is significant because it leads to larger network gaps and increases the potential for threats. For example, a company may engage an auditor for two weeks to review its financial records. The auditor gains access to sensitive data

through their work machine, which is not connected to the corporate VPN. An adversary detects this connection within the network and exploits it to move laterally, gaining persistence in the targeted environment and/or infiltrating another environment (the contractors) to compromise a secondary network, known as third-party compromise.

Furthermore, as organizational turnover increases, so do theft of intellectual property and sensitive data, as well as system sabotage (DTEX i3, 2023). Many organizations have faced the threat of disgruntled and frustrated employees exposing vulnerabilities. Additionally, malicious insiders with elevated system access may be recruited by threat actors to carry out attacks, especially when experiencing financial difficulties or workplace frustrations (Fagade et al., 2017; Woods & Allspaw, 2020).

Threat actors are adept at exploiting the personalities of potential targets or victims, instilling fear and urgency to mislead individuals into clicking a malicious link or disclosing sensitive information, thereby initiating a network breach (Akdemir & Yenal, 2021; Pranggono & Arabo, 2020). The COVID-19 pandemic exposed how the changing technological landscape, coupled with heightened public emotions, has created opportunities for threat actors to gain easy access (Akdemir & Yenal, 2021; Pranggono & Arabo, 2020). With individuals working from home, increased stress and anxiety levels among employees, and businesses rapidly adapting to technological demands, motivated offenders have taken the chance to launch sophisticated cyber-attacks (Akdemir & Yenal, 2021; Pranggono & Arabo, 2020). Generative AI has further enhanced threat actors' ability to social-engineer their way into a network (CrowdStrike, 2025). A 2024 study found that click-through rates for AI-generated phishing emails were more than 50% higher than those for human-written phishing emails (CrowdStrike, 2025).

Remote working environments have increasingly relied on cloud-based platforms to facilitate both real-time and asynchronous tasks. The large amount of sensitive data stored in the cloud has made it more vulnerable to potential threats (Khando et al., 2021; Pranggono & Arabo, 2020; Wang et al., 2020). Consequently, threat actors have adapted by becoming known as "cloud-conscious" (CrowdStrike, 2025). In fact, COVID-19-related phishing emails surged by 600% in the first quarter of 2020 alone, demonstrating how threat actors respond to changing situations (Pranggono & Arabo, 2020). During the COVID-19 pandemic, hospitals often operated on unsupported or end-of-life software and operating systems, unable to keep pace with technological advancements, making them prime targets for threat actors to launch high-impact ransomware attacks (Pranggono & Arabo, 2020).

Another emerging sub-theme in the literature on workplace adaptation is the discussion of personal devices. Employees increasingly rely on personal computers, laptops, and mobile devices to perform work tasks, store sensitive data, and access work networks (Ameen et al., 2021; Pranggono & Arabo, 2020). By their nature, personal devices are unsecured and often lack industry-standard security measures, such as strong password policies, regular updates for operating systems and browsers, and enabled monitoring tools like Endpoint Detection and Response (EDR) software (Pranggono & Arabo, 2020). The use of personal devices for work necessitates a closer examination of how workplace security standards and practices may inadvertently facilitate threat actors' intrusion methods (Ahmad et al., 2019; Ameen et al., 2021; Pranggono & Arabo, 2020). For example, an employee might receive a personal text or see a social media post prompting them to download an application that turns out to be a malicious app (Akdemir & Yenal, 2021). This can create an entry point into the targeted network for the threat actor. Moreover, remote employees are more likely to ignore security protocols due to

inconvenience (Furnell & Shah, 2020). When employees use personal devices for work tasks, organizations face increased risk of losing control over employee behavior and the technologies in use, such as firewalls, VPNs, and other safeguards, leaving sensitive data more vulnerable to breaches (Ahmad et al., 2019; Furnell & Shah, 2020).

Woods and Allspaw (2020) suggest that human factors play a critical role in security and organizational operability, more so than is widely recognized among tech firms and scholars. Although system failures, cyber-attacks, and data breaches are often attributed to technical weaknesses, researchers indicate that interpersonal dynamics contribute even more significantly to these incidents due to increasingly complex systems and interconnectivity (Cusack & Adedokun, 2018; Ma, 2021; Woods & Allspaw, 2020). Furthermore, Woods and Allspaw (2020) state that users of complex technical systems either adapt or become frustrated, which can lead to poor security practices. For instance, end users frequently use weak or reused passwords that can be easily guessed or cracked by hacking software (Kennison et al., 2021; Kennison & Chan-Tin, 2021).

Cyber intrusions are increasingly adopting a “hands-on” or “interactive” approach, in which threat actors actively engage in attacks on the targeted environment rather than relying on automated scripts or malicious code (CrowdStrike, 2024). This method gives attackers greater control over their attacks, allowing them to navigate the environment and perform reconnaissance while often blending in with routine business activities, ultimately enabling more significant attacks (CrowdStrike, 2024). As the threat actor carries out reconnaissance, they can establish heightened persistence and move laterally within the environment, exploiting potential oversights and complexities related to human vulnerabilities (CrowdStrike, 2024; Cusack & Adedokun, 2018; Kennison & Chan-Tin, 2021).

An important component to consider is the culture surrounding threat actor activity, which includes information sharing, skill development, a lack of ethical awareness, and admiration for other hackers (Christen, Ranbaduge & Schnell, 2020; Klimburg-Witges & Wentland, 2021; Romagna, 2019; Tanczer, 2019; Votipka et al., 2021). For instance, in otherwise benign contexts where information about security vulnerabilities, techniques, and tools is shared, such as online independent forums for individuals interested in cybersecurity, this information can be exploited by hackers to develop their intrusion methodology, particularly when combined with specific personality traits, such as those found in the Dark Triad (Christen, Ranbaduge & Schnell, 2020; Tanczer, 2019; Warikoo, 2021). Normative security activities, such as capture-the-flag competitions or participation in security-focused social networking groups, may lead a threat actor to engage in exploitative behavior for personal gain. This is especially likely if the individual is financially strained or confronting barriers to personal goals (Christen, Ranbaduge & Schnell, 2020; Klimburg-Witjes & Wentland, 2021; Maimon et al., 2017; Votipka et al., 2021). Cultures among threat actors typically lack ethical and legal awareness and promote admiration for underground figures, significantly contributing to practices related to cyber-attacks and cyber threats (Romagna, 2019). For example, within security hacking cultures, individuals may employ deceit and manipulation to recruit others to assist in cyber-attacks, inadvertently leading them to engage in illegal activities without fully understanding the ramifications of their actions (Romagna, 2019). Similarly, groups that idolize underground figures can create subcultures and countercultures that romanticize illegal hacking practices, attracting individuals who feel disenchanted with mainstream culture or seek social belonging elsewhere (Klimburg-Witjes & Wentland, 2021; Petry, 2011).

It is also argued that public attribution influences threat actors' choice of intrusion methodology, and there is often debate over the significance of declaring attribution (Warikoo, 2021). Attribution is the process of linking a specific originator, whether a threat actor, group, or nation-state, to a cyber-attack, based on data collected from the malicious activity, including how it occurred, the technical methodology involved, and who the target or victim was during the attack (Romanosky & Boudreaux, 2021; Warikoo, 2021). Understanding the modus operandi of threat actors is challenging to study, as these actors can leave misleading evidence that obscures the true attribution of their affiliation or mimic another cyber threat group (Romanosky & Boudreaux, 2021; Jajodia et al., 2015; Strom et al., 2018; Warikoo, 2021).

The government aims to attribute attacks to deter individuals from engaging in these activities, fearing future indictment (Romanosky & Boudreaux, 2021). However, this approach may not be an effective mechanism for deterring cybercrime. A threat actor's personality and desire for recognition can enhance their actions, providing the positive attention they may seek through their cyber-attacks or contributing to the romanticization of these actors by copycats and script kiddies who wish to emulate them (Klimburg-Witjes & Wentland, 2021). Moreover, threat actors can monetize their methods by selling malware, software, or services to those seeking to follow in their footsteps, making attribution an important indicator of the success of their offerings in the underground marketplace (Warikoo, 2021). A threat actor with personality traits like impulsivity and aggressiveness may view attribution as a motivator for retaliation (Romanosky & Boudreaux, 2021). Conversely, attribution can associate an actor with a specific group or nation-state or provide insight into plans for future attacks. Therefore, choosing tactics that might reveal attribution can endanger the threat actors themselves, their anonymity, and their attack plans (Sailio et al., 2020; Warikoo, 2021). Corporations intending to prosecute a threat

actor following a cyber-attack must rely on Cyber Threat Intelligence (CTI) organizations or threat feeds to accurately analyze and attribute the attack to a specific individual, group, or nation-state (Warikoo, 2021). While little is known about why a threat actor may or may not seek attribution, understanding personality could help bridge this knowledge gap, shedding light on the motivations behind their intrusion decisions.

Understanding threat actor personalities and intrusion decisions is essential for cybersecurity defenses, yet research remains limited. Studies indicate that insider threats are more prevalent among individuals with Dark Triad personality types (Maasberg, Warren, & Beebe, 2015), particularly those who exhibit a lack of empathy and disregard workplace norms (Maasberg, Warren, & Beebe, 2015). Furthermore, the Dark Triad can manifest in self-promoting, malicious, manipulative, and exploitative behaviors (Yin et al., 2023). This is concerning, as an insider potentially possesses insight into the vulnerabilities and gaps that exist within an organization's environment, possesses heightened credential privileges, and has knowledge of crucial assets, or might use their manipulative and exploitative tactics to acquire that intelligence (Kaya et al., 2023; Yin et al., 2023). Understanding the intrusion methodology beyond the technical context is critical for the proactive management of future cyber threats. There is a need to gain a holistic view of the decisions that threat actors use to enhance overall protection in the ever-expanding technological landscape (Belfadel et al., 2022; Georgiadou et al., 2021).

Theoretical Frameworks

It is challenging to study the personalities of individuals who engage in cyber intrusion behaviors and understand how these personalities correlate with their chosen tactics, techniques, and procedures (TTPs) (Jones et al., 2021; Jones, 2022). Respondents may provide inaccurate or

inauthentic answers about their intrusion methods, or they may misrepresent their behavior to conceal their connections to threat-acting groups and maintain anonymity (Romanosky & Boudreaux, 2021; Jajodia et al., 2015; Strom et al., 2018; Warikoo, 2021).

Evaluating theoretical frameworks can help identify the most suitable methodology for understanding hackers' behaviors and TTP selections. Frameworks promote a deeper understanding of cyber threat actors' actions, characteristics, and motivations, offering a nuanced perspective on the behaviors under study (Neufeld, 2023; Holt et al., 2016; Holt et al., 2019). The primary advantage of using a framework is that it can uncover insights that might otherwise be overlooked.

Unified Theory of Acceptance and Use of Technology

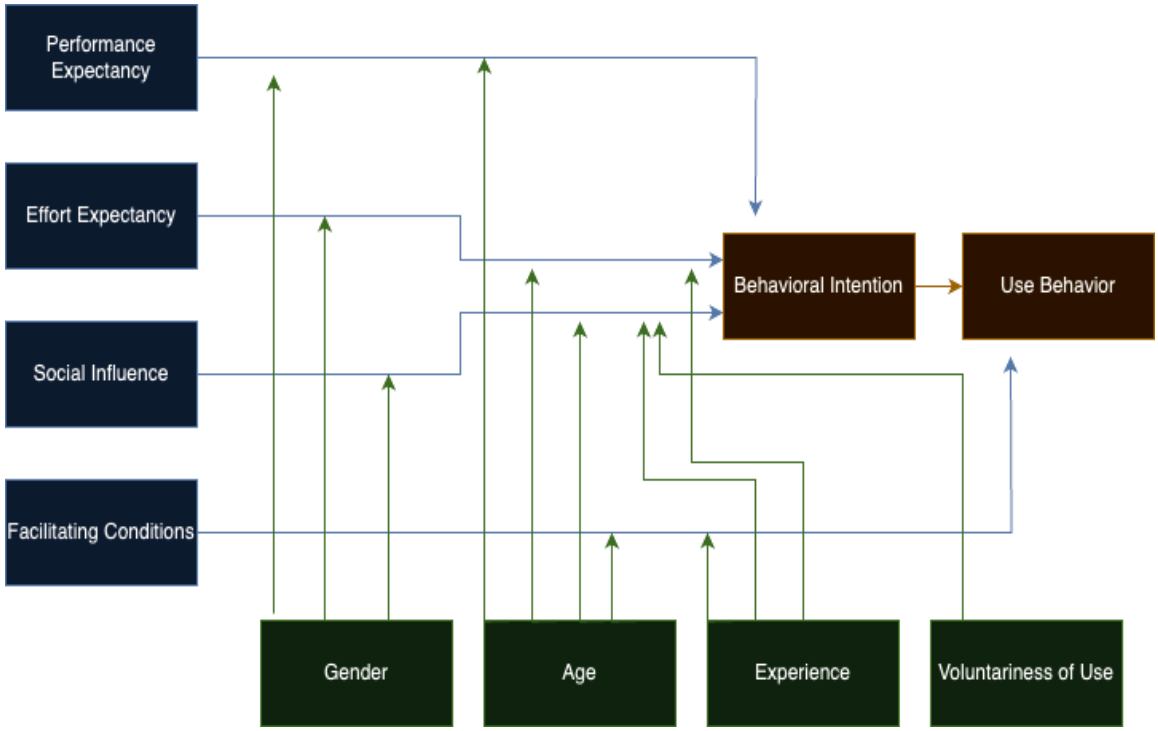
Hackers represent a complex and challenging demographic to analyze; therefore, a theoretical framework can provide a structured approach to understanding and explaining various behaviors (Angeles et al., 2013). For instance, as technology continues to evolve, employing frameworks such as the Unified Theory of Acceptance and Use of Technology (UTAUT) and its updated version, UTAUT2, can improve the ability to predict behavior and technology adoption (Bakelants et al., 2022; Venkatesh et al., 2012). Moreover, using a modeling framework for the study, the reported TTPs can be systematically categorized, enabling a comprehensive analysis of personality, behaviors, and their relationship to technological variables (Ahmed et al., 2022; Yeboah-Ofori & Islam, 2019). However, the drawback is that the cyber threat landscape is constantly evolving, which may cause models to become outdated rapidly, leading to gaps in understanding and potentially overlooking some behaviors (Kim et al., 2018; Tatam et al., 2021).

UTAUT provides a framework for understanding the factors that lead to technology acceptance and use (Ahmad et al., 2021; Venkatesh et al., 2012). These factors include

performance and effort expectancy, social influences, and other facilitating conditions (Ahmad et al., 2021; Venkatesh et al., 2012). Moderators (gender, age, experience, and voluntariness of use) influence the factors that combine to explain behavioral intention and use (Ahmad et al., 2021; Venkatesh et al., 2012). Prior research has used this framework to examine the acceptance of technologies and their contributions to positive or negative outcomes (Ahmad et al., 2021; Venkatesh et al., 2012).

Figure 1.

UTAUT Flowchart – Adapted from Ahmad et al. (2021)

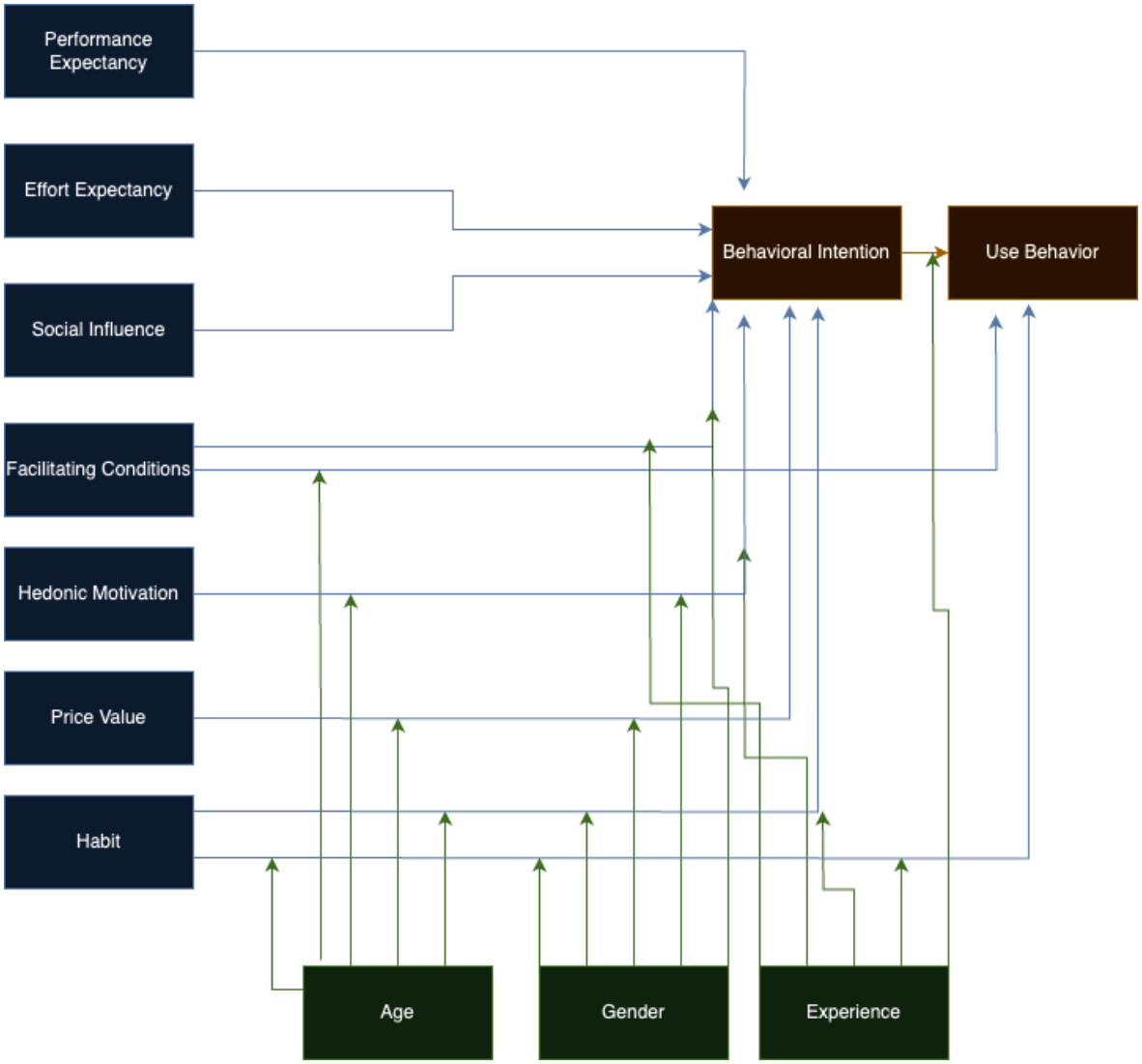


As shown in Figure 1, it is theorized that performance, effort, social influences, and facilitating conditions directly contribute to behavioral intentions (Ahmad et al., 2021). Behavioral intention dictates behavior. However, the moderators (gender, age, experience, and voluntariness) influence behavioral intention.

UTAUT was expanded into UTAUT2, incorporating hedonic motivation, price value, and habit, as shown in Figure 2 (Venkatesh et al., 2012). The enhanced factors in UTAUT2 enable researchers to gain insight into darker motivators (Raywood-Burke et al., 2021; Venkatesh et al., 2012). Prior research has attempted to understand the social dynamics of those engaging in cyber threat behavior and how knowledge is created and shared within this community (Abbasi et al., 2014; Matheus & Sarma, 2015). Under UTAUT2, the contributing factors and moderators can be used to obtain greater insight into those social dynamics.

Figure 2.

UTAUT2 Flowchart - Adapted from Venkatesh et al. (2012)



The models facilitate understanding of who is more likely to engage in technical behaviors based on the variables and factors presented (Abbasi et al., 2014). With UTAUT2, 7-point Likert-type scales are utilized, where respondents choose between strongly disagree and strongly agree; however, this method has also been adapted to a 100-point Likert scale, with 0 indicating strongly disagree and 100 indicating strongly agree (Raywood-Burke, 2021; Venkatesh et al., 2012). Age is recorded in years as reported by the respondent, gender is coded

as 0 for women and 1 for men, and experience is quantified using the actual numbers provided by respondents (Venkatesh et al., 2012). The survey questionnaire features items related to the aforementioned factors, such as “I find mobile Internet useful in my daily life.” (Venkatesh et al., 2012). When applying UTAUT and UTAUT2, partial least squares can be employed to test the models (Venkatesh et al., 2021). Spearman’s rank 2-tailed correlations and Cronbach’s Alpha can be applied for statistical analysis (Raywood-Burke, 2021).

Theory of Planned Behavior

The Theory of Planned Behavior helps to understand individuals' intent and willingness to engage in intrusive behavior (Maasberg et al., 2015). It sheds light on the influences and triggering events that lead people to take specific actions (Maasberg et al., 2015). This theory has been applied to study the Dark Triad personality traits (Maasberg et al., 2015), helping to clarify the initial motivators of hacking behavior, such as workplace dissatisfaction or financial difficulties (Maasberg et al., 2015). Certain personality traits can directly relate to intention and forecast future hacking behaviors (Maasberg et al., 2015). Implementing this framework would require multiple scales and items to assess the motives behind hacking behavior. The benefit of this approach is understanding what drives individuals, beyond their personality traits, to engage in such behaviors; however, it may increase the complexity of overall data analysis.

Capability Means Opportunity

The Capability Means Opportunity (CMO) framework is widely accepted for researching insider threats and understanding how cyber-attacks occur (Gaia et al., 2020; Maasberg et al., 2015). This framework could be applied to the dissertation study to analyze the factors that enable a successful hacking incident. Within this framework, a potential threat actor must have

the capability, motive, and opportunity to carry out the intrusion (Gaia et al., 2020). Like the Theory of Planned Behavior, CMO can offer insights into the factors that contribute to cyber threats. CMO facilitates a correlation between the means and opportunities to execute the attack, as well as the motivations behind it (Gamachchi & Boztas, 2017). One advantage of integrating the CMO is that it enhances understanding of key indicators of potential intrusion behaviors, including skill sets, experience levels, insider access, and exploitable vulnerabilities (Berndt & Ophoff, 2022; Kure et al., 2022; Mohammad et al., 2019). Implementing CMO could enhance proactive defenses and provide recommendations for advanced access controls and effective patch management policies and procedures (Berndt & Ophoff, 2022; Kure et al., 2022; Mohammad et al., 2019). A notable limitation is that this framework may require ongoing support to adapt to the continuously evolving nature of cyber threats, leading to frequent modeling updates and challenges in data collection (Tang et al., 2023).

Routine Activity Theory

Routine Activity Theory (RAT) is a framework for understanding the conditions that lead to cyber intrusions (Rege, 2013). RAT proposes that deviant opportunities arise from the routine activities of daily life, which create conditions that enable illegal activities, such as a lack of oversight and access to suitable targets (Drawve et al., 2017). Previous research has used RAT to explore the motivations behind individuals' involvement in harmful cyber activities (Burruss et al., 2021; Holt et al., 2020). Drawve et al. (2017) applied RAT to examine the motivations, target suitability, and influences on past offenders. This study reviewed nearly 250,000 assault incidents, analyzing the characteristics of offenders, victims, and offenses reported in the National Incident-Based Reporting System (NIBRS). The researchers coded the data using a binary approach, assigning 1 for yes or 0 for no regarding whether an arrest was made, if the age

range was between 15 and 55 years, and other factors, as well as the incident's timing (between 6 pm and 7 am or otherwise), the nature of the relationship (stranger or known), along with gender and race. This binary coding supports a quantitative methodology, enabling statistical analysis. Logistic regression was employed to predict the likelihood of arrest for assault. While this model may help understand the chances of engaging in certain criminal activities, a significant limitation is that no comparable dataset exists for hacker demographics and online intrusion behaviors.

Under the frameworks, content feature extraction and interaction coherence analysis can be performed to understand what people are discussing on hacker forums and categorize these discussions for statistical analysis (Abbasi et al., 2014). Data clustering, linguistic analysis, and even case studies can offer valuable insights into hacking behaviors. However, obtaining the data necessary for a comprehensive understanding of the behaviors and intentions would require access to the specific locations where individuals discuss intrusion behaviors. Due to the clandestine and covert nature of hackers, these conversations are seldom, if ever, conducted in a public forum that observers can easily access (Benjamin et al., 2015; Perkins et al., 2022).

Integrated Personality Framework for Cyber Intrusion Decision-Making

This study is grounded in an integrated personality framework that combines the Big Five personality traits and the Dark Triad to explain individual differences in cyber intrusion decision-making (Table 4). Rather than treating these models as competing explanations, the present research conceptualizes them as complementary dimensions that capture distinct yet interacting components of behavior (Costa & McCrae, 1992; Paulhus & Williams, 2002).

Table 4.

Conceptual Framework Linking Personality Traits to Cyber Intrusion Decision-Making

Personality Model	Trait	Core Psychological Function	Expected Influence on Intrusion Behavior	Representative Intrusion Behaviors
Big Five	**Openness**	Cognitive flexibility, curiosity, tolerance for ambiguity.	Promotes exploratory, adaptive, and innovative approaches.	Creative tactics, unconventional access paths, tool experimentation.
	Conscientiousness	Planning, organization, self-discipline.	Encourages methodical, structured, and low-noise approaches.	Reconnaissance, structured intrusion phases, stealth-oriented actions.
	Extraversion	Assertiveness, social engagement, action orientation.	Increases likelihood of direct, socially interactive, or visible tactics.	Social Engineering, bold engagement, initiative-taking behaviors.
	Agreeableness (Low)	Reduced empathy, competitiveness, norm resistance.	Facilitates independence and reduced social restraint.	Aggressive tactics, lateral movement, boundary-pushing behaviors.
	Neuroticism	Emotional reactivity, stress sensitivity.	May intensify persistence or reactive behavior under pressure.	Repeated attempts, fixation on access, stress-driven persistence.
Dark Triad	**Machiavellianism**	Strategic manipulation, calculated deception.	Drives deceptive, goal-oriented, and risk-calculated tactics.	Social Engineering, impersonation, credential exploitation.
	Psychopathy	Fearlessness, emotional detachment, persistence.	Drives deceptive, goal-oriented, and risk-calculated tactics.	Persistent attacks, bold actions, disregard for detection.
	Narcissism	Dominance, confidence, status-seeking.	Motivates impact-driven or visibility-oriented intrusions.	Ransomware, high-impact targeting, control-oriented behaviors.

The Big Five traits represent broad, normative dimensions of personality that shape cognitive style, emotional regulation, and behavioral organization (Costa & McCrae, 1992; Goldbert, 1993). Traits such as Conscientiousness and Openness influence how individuals plan, structure, and adapt their actions, while Extraversion, Agreeableness, and Neuroticism shape social engagement, inhibition, and stress responsiveness (John & Srivastava, 1999).

In contrast, the Dark Triad traits capture socially aversive motivational tendencies, including dominance, manipulation, emotional detachment, and risk tolerance (Jones & Paulhus, 2014; Paulhus & Williams, 2002). Machiavellianism reflects strategic deception and the pursuit of long-term goals. Psychopathy is reflected in fearlessness and persistence under threat. Narcissism reflects status-seeking and confident behaviors. These traits are theorized to influence individuals' pursuit of certain intrusion strategies, especially those involving deception, persistence, and high-risk tactics (Curtis et al., 2018; Jones et al., 2021).

The Big Five and the Dark Triad together create a dual-pathway model: normative personality traits influence the cognitive and procedural approaches to intrusion, whereas dark traits determine motivation levels, ethical limits, and risk preferences (Gaia et al., 2022). Thus, cyber intrusion decision-making is viewed as the outcome of an interplay between behavioral regulation and inherent motivations, rather than solely technical ability.

The integrated framework shaped the study’s hypotheses, helped interpret both quantitative and qualitative results, and served as the foundation for linking personality traits to observed intrusion behaviors. By explicitly merging these personality models, the research promotes a more complete understanding of how individual differences affect the nature and purpose of cyber intrusions.

Summary

Personality and behaviors are highly complex and nuanced (Haz et al., 2022; Maasberg et al., 2020; Vedel & Thomsen, 2017; Wang et al., 2022). The intersection of the Dark Triad with the Big Five provides insight into trait connections and how specific trait combinations can predict behavioral expressions (Garcia & Moraga, 2017). In particular, when examining which model better predicts hacking behavior, the Dark Triad is often deemed a primary predictor of deviant and malevolent behaviors (Gaia et al., 2020; Gaia et al., 2022; Geel et al., 2017; Maasberg et al., 2020; Paulhus et al., 2021). No single scale can sufficiently predict whether an individual will engage in deviant and possibly unlawful activities (Gaia, 2022; Jones & Mueller, 2021; Jones et al., 2021; Tamraker et al., 2016). Several unique facets interact, such as perceptions of apprehension, Agreeableness, and situational trait activation (Gaia, 2022; Jones & Mueller, 2021; Jones et al., 2021; Tamraker et al., 2016).

Research indicates that individuals in normal ranges of the Big Five often wish to change specific personality traits, while those aligned with the Dark Triad tend not to (Baranski et al., 2017; Hudson, 2022; Hudson et al., 2019; Hudson & Fraley, 2015; Hudson & Fraley, 2016; Miller et al., 2019; Quintus et al., 2017). This distinction is essential as it highlights the necessity of maintaining two separate scales; those with general traits may resist or adjust personality characteristics that veer toward darkness, whereas individuals exhibiting dark traits typically intend to preserve those qualities (Baranski et al., 2017; Hudson, 2022; Hudson et al., 2019; Hudson & Fraley, 2015; Hudson & Fraley, 2016; Miller et al., 2019; Quintus et al., 2017). This understanding can aid in creating personality profiles for hackers and analyzing the correlation of their attack methods, whether loud or stealthy (Jones et al., 2021; Garcia & Moraga, 2017).

Researchers emphasize that personality assessments, such as the Big Five or the Dark Triad, have limitations that should be acknowledged and discussed in light of individual research

objectives (Soutter et al., 2020). Prior studies on cybersecurity and the Big Five have not yet explored the relationship between intrusion behaviors and the personality traits of threat actors (Budimir et al., 2021; Kennison & Chan-Tin, 2021; Troisi et al., 2020). While earlier research suggests that certain personalities within the Big Five, such as Openness, might increase the likelihood of engaging in threat actor behaviors (Budimir et al., 2021), other studies refute this by claiming that Agreeableness serves as an indicator while Openness is associated with victimization (Fagade et al., 2017).

A synthesis of the literature explored in this chapter reveals several gaps in existing research regarding how personality characteristics contribute to cybersecurity threats and intrusion behaviors (Harms et al., 2022). Predicting behaviors based on personality types and traits can significantly enhance proactive defenses (Basak et al., 2018; Curtis et al., 2021; Jones et al., 2021; Jones, 2022). Understanding an individual's unique personality profile and its influence on hacking tendencies can facilitate early intervention, potentially altering specific traits before they develop into malicious characteristics (Kioskli & Polemi, 2020; Xu et al., 2013). For instance, boosting Agreeableness has been shown to reduce the prevalence of Dark Triad traits (Hudson, 2022).

The need for innovative strategies to keep pace with the changing threat landscape is not merely suggested; it is essential (Basak et al., 2018; Curtis et al., 2021; Verizon, 2024). Grasping the unique patterns of personality, particularly the dark traits that lead to deviant cyber behaviors, can establish a strong, proactive defense mechanism for organizations (Basak et al., 2018; Curtis et al., 2021; Jones et al., 2021). While the MITRE ATT&CK matrix serves as a comprehensive technical resource for defenders, the consideration of personality remains a crucial missing element in defense strategies (Al-Shaer et al., 2020; Curtis et al., 2021; Georgiadou et al., 2021;

Jones et al., 2021; Straub, 2020). Given the evolving nature of cyber threats, defense strategies must adapt to incorporate the human element in attacks (Jones et al., 2021).

METHODOLOGY

This chapter outlines the research methodology and study design. The main focus of the analysis was on exploring the relationship between Dark Triad personality traits and cyber intrusion decision-making (RQ1). The Big Five personality traits (RQ2) were also analyzed to provide additional insights into broader cognitive, emotional, and behavioral patterns that contextualize intrusion behavior.

A mixed-methods, non-experimental research design was employed, combining quantitative survey data with qualitative responses to open-ended, scenario-based questions. This approach allowed for both statistical analysis of trait-behavior relationships and a more in-depth exploration of the reasoning participants described when conceptualizing cyber intrusion strategies.

The following sections describe the data collection procedures, recruitment strategy, operationalization of variables, design of the MITRE ATT&CK-based scenario, and the analytical methods used to analyze both quantitative and qualitative data.

Research Method and Design

This study used a convergent mixed-methods design, collecting and analyzing both quantitative and qualitative data simultaneously to gain a comprehensive understanding of intrusion methodology in relation to personality typology. The goal was to gather qualitative insights that complement and deepen the interpretation of the quantitative findings.

Quantitative analyses examined statistical links between personality traits and intrusion behaviors, while qualitative thematic coding detailed participants' thoughts about the intrusion scenario. These two data streams were integrated during interpretation, with qualitative

narratives clarifying indirect effects, explaining non-significant quantitative results, and demonstrating how personality traits manifested in potential intrusion situations. This method promotes triangulation and enhances the validity of the results.

Although mixed-methods surveys are often considered difficult to carry out, this approach was selected because it offers a comprehensive and nuanced understanding of the issue (Ivankova et al., 2006; Roer-Strier & Kuram, 2009; Saldaña, 2015; Scott & Briggs, 2009; Usman et al., 2021). However, poor planning and preparation for a mixed-methods design could lead to "argumentative incoherence," a challenge that was addressed during the study's design and implementation (Scott & Briggs, 2009). Because the hacker population is a complex demographic to study, the goal was to use respondents' time efficiently by leveraging the strengths of both closed- and open-ended questions.

The benefit of using a mixed-methods design is that it combines survey responses with direct participant responses, which helps achieve a deeper understanding (Hadi et al., 2012; Roer-Strier & Kuram, 2009). Mixed-methods can deliver more comprehensive and insightful results than either method alone (Anwar, 2015; Mills et al., 2012; Roer-Strier & Kuram, 2009).

A limitation of mixed-methods designs is that the analysis can become more complex, which may lead to reporting challenges (Ivankova et al., 2006; Scott & Briggs, 2009). With this in mind, open-ended responses were coded thematically using a pre-designed codebook (Roer-Strier & Kuram, 2009; Saldaña, 2021). The full qualitative codebook, including category definitions, examples, and coding procedures, is provided in Appendix B. The coding process required researchers to interpret the meanings of specific sentiments while remaining adaptable and flexible during analysis to avoid unintentionally omitting valuable information or misrepresenting responses (Glazier et al., 2021; Spector & Pinto, 2015).

Within qualitative data analysis, research bias is a common risk. As noted by Glazier et al. (2021), codebooks must accommodate variable responses, be dynamic, thorough, and rigorously tested. For this reason, the codebook was reviewed by other security practitioners to obtain inter-rater reliability and reduce potential biases in the analysis and review.

Web-based Survey Study

Web-based surveys generally produce lower response rates than traditional in-person studies, as participation across all methods has declined, largely due to the growing number of studies causing survey fatigue (Sammut et al., 2021). Research indicates that response rates for web-based surveys range from 35% to 44% (Sammut et al., 2021; Wu et al., 2022). Traditional in-person studies often report response rates that are 11% to 13% higher than those of online studies (Sammut et al., 2021; Wu et al., 2022). Given the demographic chosen for this study, the slightly lower response rate is accepted as a limitation.

To achieve the highest response rate, best practices were implemented. Research shows that sending surveys to a larger audience does not necessarily increase completion rates; instead, targeting a clearly defined group leads to better response and completion rates (Wu et al., 2022). It is also recognized that including open-ended questions may increase attrition due to higher cognitive load (Neuert & Lezner, 2019; Saleh & Bista, 2017; Wu et al., 2022). Although cognitive demand may contribute to non-response and incomplete surveys, studies suggest that completion decreases only slightly (Neuert & Lezner, 2019). The data show that completion rates decrease by 5-10%, placing them in the 30-40% range (Neuert & Lezner, 2019).

Survey instructions and questions were clear, and the survey took about 15-20 minutes to complete, consistent with participants' preference for surveys under 15 minutes (Neuert & Lezner, 2019; Saleh & Bista, 2017; Sammut et al., 2021). The study intentionally limited the use

of open-ended questions to reduce overall cognitive load (Neuert & Lezner, 2019). Research shows that interest in the topic and assurances of confidentiality can increase response rates, so participants were recruited based on their interest and assured of confidentiality and anonymity (Saleh & Bista, 2017).

Data Collection

The sample for this study included individuals involved in or familiar with cybersecurity. The goal was to gather a diverse range of participants, including officially employed cybersecurity professionals and informal participants from the broader hacking and information security communities. To ensure responses were relevant and applicable, participants had to self-identify as having experience in cybersecurity, ethical hacking, penetration testing, or related activities.

Before collecting data, the research protocol was approved by the Institutional Review Board (IRB) at Purdue University, West Lafayette (IRB-2025-964), and classified as Exempt under federal guidelines for minimal-risk research. All participants received an informed consent form explaining the study's purpose, voluntary nature, and confidentiality measures. No personally identifiable information was collected, and responses were stored securely in accordance with the university's data protection policies.

When participants opened the survey link, they were immediately provided with the research participation sheet, which outlined the study details. After reading the information, participants were asked to confirm that they agreed to participate in the research, were 18 years or older, and understood the information in the participation sheet. If they selected yes, they could proceed to the next survey phase. If they did not meet the criteria and selected no, they were directed to the end of the survey and thanked for their time.

If participants selected “yes,” they were directed to the criteria page. Participation required that they be at least 18 years old, fluent in English, and have experience in cybersecurity, ethical hacking, penetration testing, red teaming, or related technical fields. If they selected yes, they moved on to the next page. If they selected no, they were taken to the end of the survey and thanked for their time.

Participant Recruitment

While the population is inherently hard to define due to its decentralized and secretive nature, recruiting from multiple online platforms (e.g., Discord, Reddit, security forums) with strong engagement from cybersecurity communities helped to ensure a reasonably representative sample. Stratified recruitment across diverse communities, from formal professional forums to informal technical spaces, supported a varied and meaningful dataset that reflected the diversity of the hacker population.

Recruitment occurred through various cybersecurity Discord servers, Reddit pages dedicated to cybersecurity, and topical forums. These platforms are also highly active and attract a diverse range of participants. Before posting the survey to any forum or server, the researcher performed a risk assessment to ensure the study would be welcomed, safe to share, and compliant with community rules. The researcher also consistently requested moderator approval before posting in each community.

Participants were recruited through general and public messages. No direct messaging or private solicitation was ever used. The posts included the recruitment script, which featured the Purdue Qualtrics secure survey link. Screenshots of the participation and eligibility forms are provided in Appendix C to illustrate the survey flow and participant screening process.

The survey did not gather IP addresses, usernames, or any other PII. This was intentionally done to safeguard the participants' anonymity. Additionally, the researcher did not collect any usernames or PII from individuals who commented on the survey posts or sent messages to the researcher.

The Qualtrics anonymization settings and bot-prevention tools (e.g., reCAPTCHA) were enabled. Participants were informed about these safeguards in the recruitment message and the informed consent section of the survey.

Sample Size Justification

The sample size was determined based on statistical power considerations and the analytical demands of the mixed-methods design, which included correlational analyses, binary logistic regression, moderation testing, and exploratory machine-learning validation. An a priori power analysis was conducted using conventional parameters for behavioral research ($\alpha = 0.05$, power = 0.80), indicating that a minimum sample of approximately 180-200 participants was required to detect small-to-moderate effect sizes in multivariate regression models (Cohen, 1988; Tabachnick & Fidell, 2019).

A total of 257 participants completed the closed-ended survey, surpassing the minimum thresholds needed for stable estimation of odds ratios, interaction effects, and model performance metrics. Of these, 196 participants finished the entire study, including the open-ended simulated intrusion scenario, providing enough depth for qualitative thematic analysis.

Recruitment took place through publicly accessible online platforms and cybersecurity communities. This method was intentionally chosen to reach individuals with varying technical skills and cybersecurity knowledge while avoiding ethical, legal, and safety issues related to associagingwithith illegal or covert cybercrime networks. The goal was to include a broad range

of cognitive styles and experiences, focusing on decision-making processes rather than identifying specific malicious threat actors.

The achieved sample size offered sufficient statistical power and methodological triangulation, further enhanced by the reliability and interpretability of the study's quantitative and qualitative results.

Risk Assessment

An initial review of Discord servers and online cybersecurity communities found that not all platforms were suitable for recruitment, and some posed potential personal security risks. For example, one Discord server described itself as: "Grey-hat hacking group ExomSec conducts hacks against countries, companies, or individuals periodically. The server assists with technical problems and discusses security with anyone! Do not mess around, or there will be consequences!" While such groups may include technically knowledgeable individuals relevant to the study population, the explicit reference to coordinated hacking activity and the implied threat of retaliation suggested a heightened risk to the researcher.

To mitigate these risks, a structured risk assessment was conducted before posting the survey in any online community. Each potential recruitment platform was evaluated using predefined screening criteria to identify indicators of unsafe or illicit activity. These criteria included threats, encouragement of illegal hacking operations, hostile language toward outsiders, or explicit enforcement mechanisms against perceived misconduct. Communities exhibiting any high-risk indicators were excluded from recruitment. Table 5 presents the risk assessment questions and the corresponding actions taken for each outcome.

Table 5.

Risk Assessment

Risk Question	Response
Does the server or forum tag black hat hacking?	Yes – Be cautious. No – Proceed with risk assessment. Continue to review regardless of Yes or No.
Are there rules?	Yes – Proceed with risk assessment. No – Be cautious.
Do the rules permit posting jobs, events, and other solicitations?	Yes – Proceed with risk assessment. No – Eliminated from study.
Does the server have statements of threats towards individuals?	Yes - Eliminated from study. No – Proceed with risk assessment.
Does the server state it allows hacking towards individuals?	Yes - Eliminated from study. No – Proceed with risk assessment.
Does the server or forum function as an illegal exchange of services or materials?	Yes - Eliminated from study. No – Proceed with risk assessment.
Does the server or forum require application for admittance (i.e., it is not publicly available to view)?	Yes - Eliminated from study. No – Proceed with risk assessment.

The risk assessment was applied to all prospective recruitment locations before survey distribution. The survey was posted exclusively on publicly accessible Discord servers, Reddit communities, and forums focused on educational, defensive, or general cybersecurity discussions. Platforms requiring private admission, vetting, or closed-group access were excluded. Additionally, platforms where the risk assessment identified explicit hacking activity, threats, or retaliatory language were removed from the recruitment pool.

The screening process ensured participant outreach took place in safe, ethically appropriate environments while maintaining access to individuals with relevant cybersecurity knowledge and experience.

Recruitment Communities

Research on Discord about cybersecurity and hacking servers uncovered several groups with many members and rules that allowed the survey to be posted. It is important to note that the membership count changes constantly, as these are public servers; anyone can join at any time. A summary of Discord servers and their associated membership counts is provided in Table 6.

Table 6.

Discord Membership Sample

Discord Server Name	Classification	Membership Count
Black Hills Infosec	Infosec Community	44,544
Bounty Hunters	Bug bounty hunter community	14,293
Cyber Info	Educational	10,212
Hacker101	Educational	76,300
HACKERverse	Hacker Community	4,402
OffSec	Offensive Security Community	55,014
SANS Offensive Operations	Educational	11,118
TryHackMe	Ethical Hacker Community	267,500
WhiteHat Hacking	WhiteHat Community	34,678

Like Discord, Reddit has multiple dedicated Subreddits focused on cybersecurity, hacking, and related interests. Table 7 lists the Subreddits and their membership counts. A risk assessment was also conducted before posting the survey in any Reddit community. These communities have rules about what is appropriate to post and what will be removed, which may result in a ban.

Table 7.

Reddit Community Sample

Reddit Community	Membership Count
r/cybersecurity	1.1 million
r/CyberSecurityJobs	38,000
r/CyberSecurityAdvice	62,000
r/hacking	2.8 million
r/Hacking_Tutorials	328,000
r/Hacking_Tricks	38,000
r/HowToHack	429,000
r/Pentesting	47,000
r/theHackerguide	128,000
r/WebExploits	137,000

As shown in the tables for the Discord (Table 6) and Reddit (Table 7) communities, there are potentially millions of individuals to tap into for the study. It is essential to note that people often join multiple servers and communities of interest, and there is no straightforward way to remove duplicate memberships.

Design

Once the survey was posted, potential participants were directed to a secure Purdue Qualtrics link. Given the participants' nature and tendency to be wary of clicking links, the recruitment statement included assurances about the link's safety. It acknowledged that no tracking software or IP addresses would be recorded. Adequate safeguards, particularly regarding data privacy protection, were crucial (Maslej et al., 2024; Pan et al., 2023; Sebastian, 2023). Respondents of online surveys must be confident that their responses are secure and that their privacy is of top concern (Kasneci et al., 2023; O'Neill & Connor, 2023; Sebastian, 2023; Yan et al., 2023).

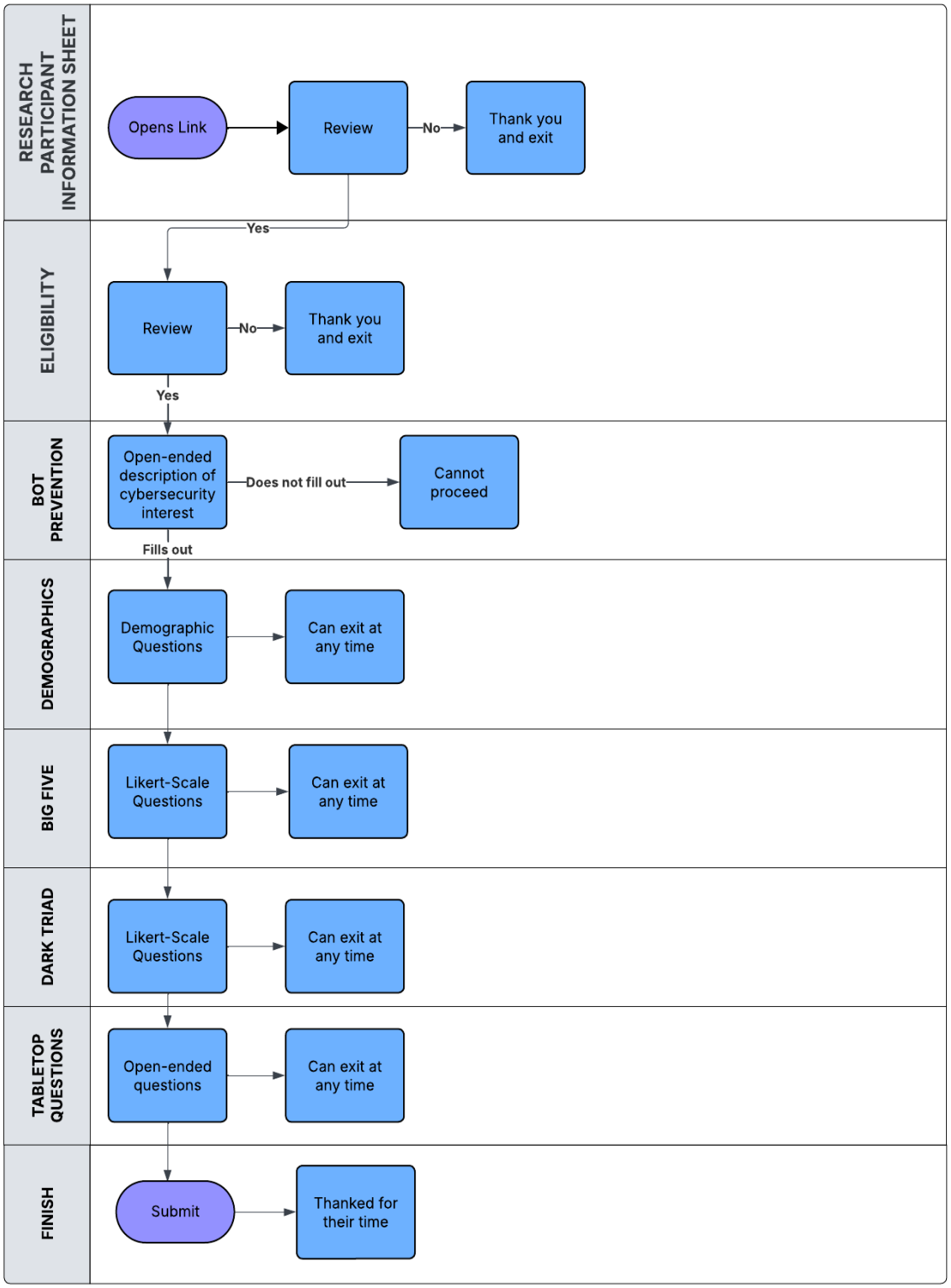
The researcher was cautious about potential risks from survey bots. Bot detection features were enabled, and any response flagged by Qualtrics as suspicious was flagged. However, it is important to note that Qualtrics often identified responses as bots due to the open-ended questions about hacking techniques. Upon review, the system was found to recognize responses that used specific hacking terminology. Therefore, each response was carefully examined to confirm that it was written by a human. Responses that seemed to be generated by a bot were removed from the study.

To further eliminate potential bot responses, the first question after the informed consent and inclusion criteria was an open-ended response asking the participants to outline their interest in the field.

After completing the initial steps, participants moved through a structured series of survey components. The study flow is depicted in Figure 3, which shows each stage from submission entry. Once they reviewed the participation information sheet and confirmed eligibility, respondents answered an open-ended screening question designed to verify genuine interest in cybersecurity. This aimed to prevent automated or non-human responses. Those who did not provide a valid open-ended answer were screened out of the survey and could not continue.

Figure 3.

Study Flow



Eligible participants then proceeded to the main sections of the questionnaire, beginning with demographic questions, followed by the Big Five Inventory and the Short Dark Triad (SD3) personality assessments. Each section allowed respondents to exit at any time without penalty. The final part of the survey included open-ended tabletop exercise questions to gather qualitative data on decision-making processes during simulated intrusion scenarios.

Participants could complete the study using either a desktop browser or a mobile device. At the end of the survey, all respondents were thanked for their time and instructed to submit their responses. This step-by-step design ensured a logical and secure flow of participation while maintaining data integrity and participant autonomy.

At the beginning of the Big Five Inventory and the Dark Triad, instructions were presented for the participant to review, guiding them in answering the questions. After completing all Likert-type survey items, the participants moved to the final section, which consisted of the open-ended responses. After completing the responses, participants were thanked for their time.

Data was collected from July through August 2025. Once data collection was complete, the survey link was closed, preventing further participation in the study.

Demographic Questions

The demographics section consisted of eight questions drawn and adapted from the Qualtrics Library of standard demographic items. The questions shown in Table 8 were selected to collect general background information without requesting any personally identifiable information. The study examined participants' age, gender, education level, employment status, and cybersecurity involvement to provide a basic understanding of the population represented.

Question 8 was specifically modified before data collection to capture the extent of participants' engagement in cybersecurity, including whether they were formally employed in the field, self-taught, or involved in hacking or penetration testing activities. This modification was implemented to contextualize the sample better and examine whether experience and involvement influenced behavioral and personality-based outcomes. All responses were optional, and no questions required disclosure of identifying information.

Table 8.

Demographic Questions

Q1 How old are you?	Age slider
Q2 What is the highest level of school you have completed or the highest degree you have received?	Less than high school degree High school graduate (high school diploma or equivalent including GED) Some college but no degree Associate degree in college (2-year) Bachelor's degree in college (4-year) Master's degree Doctoral degree Professional degree (JD, MD)
Q3 How do you describe yourself?	Male Female Non-binary / third gender Prefer to self-describe
Q4 Choose one or more races that you consider yourself to be:	White Black or African American American Indian or Alaska Native Asian Native Hawaiian or Pacific Islander Other
Q5 Are you of Spanish, Hispanic or Latino origin?	Yes No
Q6 What is your current marital status?	Married Living with a partner Widowed Divorced/Separated Never been married
Q7 Which statement best describes your current employment status?	Working (paid employee) Working (self-employed) Not working (temporary layoff from a job) Not working (looking for work) Not working (retired) Not working (disabled) Not working (other) Prefer not to answer
*Q8 – **Original question** What is your approximate salary?	Less than $10,000 $10,000 to $19,999 $20,000 to $29,999 $30,000 to $39,999 $40,000 to $49,999 $50,000 to $59,999 $60,000 to $69,999 $70,000 to $79,999 $80,000 to $89,999 $90,000 to $99,999 $100,000 to $149,999 $150,000 or more
Q8 – **New question** Which of the following best describes your current involvement in cybersecurity or hacking-related activities? Select the option that most closely aligns with your experience.	Hobbyist Student Aspiring professional Professional penetration tester Security researcher or bug bounty hunter Security Professional in Leadership or Academia System Administrator or IT Professional with security responsibilities. Other: please specify

Big Five Inventory

The study used the Big Five Inventory from the Berkeley Personality Lab, shown in Figure 4 (John, Donahue, & Kentle, 1991; John, Naumann, & Soto, 2008). The scale consisted of 44 items, in which participants could select their response on a 1 to 5 scale, where 1 represented Strongly Disagree, and 5 represented Strongly Agree. The scale demonstrated strong internal consistency, with an overall Cronbach's α of 0.83. Please see Appendix D for the full Big Five Inventory.

Dark Triad

Upon completion of the Big Five, participants could then proceed to the Dark Triad questionnaire. The Short Dark Triad (SD3) scale was utilized for this study (Jones & Paulhus, 2014). The SD3 consisted of 27 items, organized into three subscales assessing Machiavellianism, Narcissism, and Psychopathy. Like the Big Five Inventory, participants were able to select their response on the scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The reliability of the three subscales within the SD3 was 0.71, 0.77, and 0.80, respectively (Jones & Paulhus, 2014). The full scale is in Appendix D.

Tabletop Portion

After completing the demographics, Big Five, and SD3 assessments, the participant moved on to an open-ended section to discuss their behavior and decision-making during an attack scenario. The scenario was presented like a Tabletop Exercise (TTX) that many companies use to test cyber incident readiness and resilience.

The goal was to understand what choices the participants made regarding various tactics. They were asked to elaborate on their decisions and be specific. As they responded, additional

information about the environment and situation was provided to enable more comprehensive responses in subsequent phases. In the scenario, two closed-ended questions were presented intentionally to limit cognitive load. Appendix E provides the scenario with the open-ended questions.

Intrusion Scenario

Before the open-ended questions began, a scenario was presented for the participants to read. It depicted a large hospital in the Midwest under strain during peak sickness season. The scenario was intentionally designed to reflect a realistic operational environment, with a complex layout. The subsequent questions addressed multiple MITRE ATT&CK stages. These questions were crafted as injects, with each one introducing new information. This approach was intentionally used to mimic a tabletop exercise (TTX) typically designed in a corporate setting. Appendix E contains the scenario, injects, and questions used throughout this segment of the study.

To reduce the potential for researcher bias in the scenario, the development of the hypothetical setting and associated injects was informed through consultation with cybersecurity professionals and industry peers. These included Chief Information Security Officers (CISOs), director-level information security professionals, and penetration testers. The discussions with these industry experts helped ensure that the scenario represented a plausible enterprise environment and attack surface, rather than an artificially constructed or theoretically biased scenario.

The technical architecture of a fake hospital was explained, including details such as the operating systems used, the number of employees, and the composition of the security team. The scenario overview was clear and concise, reducing cognitive load.

Injects

The injects were also developed through consultation with industry peers. They represented Reconnaissance, Initial Access, Evasion and Persistence, Escalation, Detection, and Ransomware Deployment or Exit.

The questions guided the participants while allowing them the freedom to respond in the way they felt was best. For example, the Reconnaissance inject (Inject 1) stated that it is peak flu/COVID season, and the hospital is overwhelmed. It asked what the reconnaissance steps are and how they prioritize targets in that specific environment.

Subsequent questions followed the same method: identifying where the participant is in that specific phase, asking how they are maintaining access while avoiding detection, and, now that they have access, how they continue.

Injects 4 and 6 were both presented as closed-ended questions. This was intentional to reduce cognitive load. These two questions still followed the same pattern of having an MITRE ATT&CK-aligned phase, but provided options for participants instead of asking them to enter responses.

Operationalization of Variables

Personality constructs were measured using two validated psychometric tools, the Big Five Inventory and the Short Dark Triad. The Big Five Inventory (BFI) evaluated five major personality dimensions and was scored on a five-point Likert scale (John & Srivastava, 1999). The Short Dark Triad (SD3) assessed Machiavellianism, Narcissism, and Psychopathy (Jones & Paulhus, 2014). For both tools, higher scores indicated a stronger endorsement of the respective personality trait.

To capture the shared variance across the Dark Triad traits, a composite Dark Triad index was calculated by averaging participants' scores across the three SD3 subscales. This index provided a unified measure of overall dark personality tendencies, reducing redundancy among subscales while enabling analysis of the general "dark" dispositional effect.

Cyber intrusion behavioral variables were derived from an open-ended, scenario-based exercise. Participants were asked to describe the tactics they would employ during a hypothetical cyber intrusion. Responses were systematically coded as binary variables, with 0 indicating absence and 1 indicating presence. This coding indicated whether each behavioral category appeared in a participant's response.

The coding framework was developed from prior research and informed by the MITRE ATT&CK taxonomy. It was adapted to capture both technical and psychological dimensions of attacker behavior. Behavioral categories included boldness, deception, persistence, creativity, structure, sophistication, aggression, high-risk behavior, lateral movement, privilege escalation, ransomware, Social Engineering, and reconnaissance. This operationalization enabled the integration of qualitative behavioral data into quantitative analyses. The complete codebook and definitions of the categories are provided in Appendix B.

Data Analysis

Data analysis occurred following the collection of both qualitative and quantitative data. The dataset was reviewed for fraudulent or low-quality responses, such as identical answers across all items or nonsensical replies to open-ended questions. To ensure anonymity, participants were assigned pseudonyms (e.g., P1, P2, P3), and any identifying information embedded in responses was redacted or replaced with pseudonyms.

Open-ended responses from the MITRE ATT&CK scenario were analyzed first using a structured coding process to transform qualitative text into quantifiable variables. A binary coding scheme was developed in advance, based on the hypotheses and prior literature, to capture the presence (1) or absence (0) of specific behavioral categories (e.g., bold, deceptive, high-risk, structured, creative, persistent). The coding rubric, detailed in Appendix B, included operational definitions and keyword indicators, which ensured consistency.

The coding process followed a three-stage procedure (Saldaña, 2015):

Preparation: All qualitative responses were exported from Qualtrics and cleaned to remove formatting inconsistencies. Responses were reviewed to identify and redact any accidental disclosure of identifying information.

Keyword and Contextual Coding: Responses were examined for keywords aligned with the codebook (e.g., “brute force” → bold; “fake credentials” → deceptive). When keywords were present, the researchers also reviewed the broader context to prevent misclassification. Each behavior was recorded as binary: present (1) if the behavior appeared, absent (0) if not.

Quality Control: After the initial coding, responses were re-examined to confirm consistency across categories. Special attention was given to edge cases (e.g., behaviors that did not clearly fall into specific categories). To evaluate the reliability of the coding scheme, two independent coders, both full-time cybersecurity professionals, reviewed a randomly selected subset comprising approximately 20% of the responses. Each coder independently applied the established rubric to the responses without prior exposure to the original coding decisions.

Inter-rater reliability (IRR) was assessed using Cohen’s Kappa, which accounts for agreement occurring by chance. The resulting kappa value was $\kappa = .98$, indicating near-perfect

agreement between coders according to the interpretation guidelines established by Landis & Koch (1977).

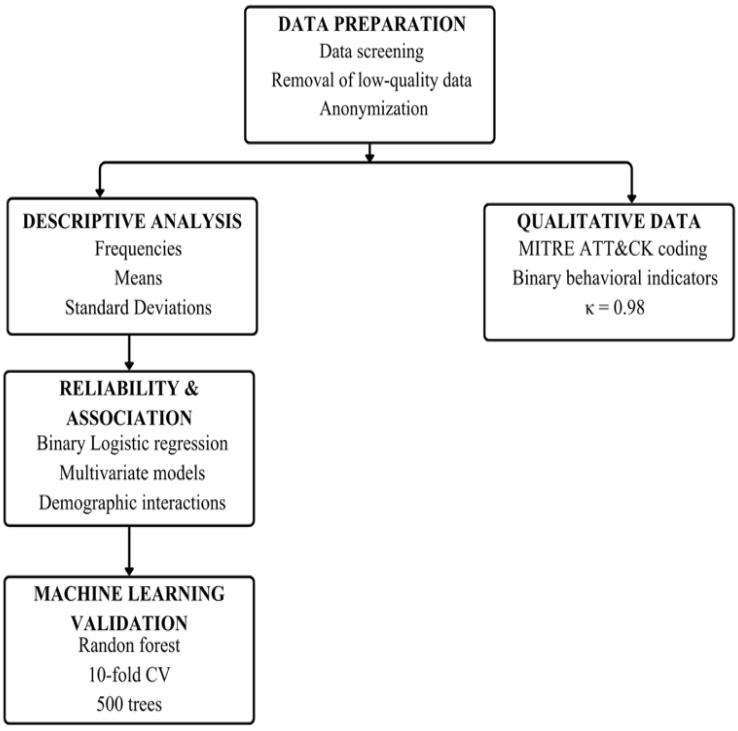
As an additional validation step, a subset of the coded responses (approximately 25%) was also compared against AI-assisted coding outputs to identify any potential inconsistencies or overlooked interpretations. The AI comparison served only as a supplementary quality check and was not used to determine the final coding classifications. Final coding decisions and IRR calculations were based exclusively on the human coders' evaluations.

This process ensured that open-ended responses were systematically reduced into analyzable binary variables. The coded data were subsequently integrated into quantitative analyses, enabling the use of logistic regression and correlation analyses to test hypotheses regarding the relationships between personality traits and cyber intrusion behaviors.

Data were analyzed using Python (v3.13). Python was chosen for its flexibility in handling large datasets and the ability to integrate both traditional statistical modeling and machine learning approaches. The analysis incorporated both quantitative and qualitative approaches, consistent with the study's mixed-methods design. The statistical analysis workflow is illustrated in Figure 4.

Figure 4.

Data Analysis Workflow



An a priori power analysis was conducted in accordance with Cohen's (1988) standards for multiple regression. Assuming a medium effect size ($f^2 = 0.15$), $\alpha = 0.05$, and power = 0.80, the minimum required sample size was calculated as 92 participants. The final sample ($n = 257$ for completion of personality tests, and $n = 196$ for completion of the entire survey) exceeded this requirement, ensuring adequate power to detect significant effects.

Ethical Considerations

This study was reviewed and approved by the Purdue University Institutional Review Board (IRB) prior to data collection (IRB-2025-964). All participants were provided electronic informed consent before beginning the survey. To ensure anonymity, no personally identifiable information (PII), IP addresses, or geolocation data were collected. Qualtrics' anonymization

features and bot-prevention safeguards (reCAPTCHA and duplicate response checks) were enabled throughout data collection.

Recruitment was limited to moderated online spaces, including cybersecurity-related Discord servers, Reddit forums, and publicly accessible forums. This approach reduced the risk of engaging in illicit or black-hat communities. No compensation was provided, and participation was voluntary, with participants free to withdraw at any time. These safeguards aligned with ethical principles of respect for persons, beneficence, and justice (Belmont Report, 1979).

Summary

This chapter outlined the methodology for investigating the relationship between personality traits and cyber intrusion behaviors. A mixed-methods, non-experimental design was used, combining quantitative survey data with qualitative scenario-based responses. The chapter detailed the research design, participant recruitment, data collection procedures, variables and operationalization, analysis plan, and ethical considerations.

The methodology ensured a rigorous examination of the primary research question regarding the influence of Dark Triad traits (RQ1) and the secondary research question examining the Big Five traits (RQ2). The integration of binary-coded qualitative data added depth to the statistical analyses, enabling a more comprehensive understanding of hacker decision-making.

RESULTS

This chapter presents the empirical results related to the study's research questions and hypotheses, using both quantitative and qualitative data. Multiple statistical techniques were used to address the research questions, including descriptive statistics, reliability tests, correlation analyses, logistic regression, and Random Forest classification. These methods were selected to provide traditional inferential insights and machine–learning–based validation of the findings. The qualitative data were further analyzed to gain a deeper understanding of the participants' narratives, offering a comprehensive view of the results.

Various statistical techniques were used to ensure the validity and reliability of the results, with each method serving a specific analytical purpose. Regression and Random Forest models provided more accurate estimates of effect size and predictive power. Agreement across these methods increases confidence in the results and underscores the study's robustness.

This chapter clearly and succinctly summarizes the key findings related to the research questions and hypotheses. It emphasizes the most significant and theoretically relevant results, particularly regression models that yield interpretable estimates of how personality traits affect outcomes, and Random Forest models that highlight the predictive strength of traits across various behaviors. Supporting analyses, such as correlations, are briefly mentioned when they substantiate the main results, while detailed data are omitted to avoid redundancy. Overall, these findings provide a clear and comprehensive overview of the relationships between the Dark Triad, Big Five personality traits, and decision-making in cyber intrusion scenarios.

Demographics

A total of 385 responses were initially collected through the survey platform. Participants who did not complete at least the Big Five and Dark Triad assessments were excluded. The dataset was further screened for data quality, and responses that appeared non-human or clearly invalid, such as nonsensical or intentionally disruptive entries, were removed prior to analysis.

After applying the inclusion criteria, the final sample comprised 257 participants. Of these, 196 completed both the quantitative personality measures and the open-ended intrusion scenario, whereas 61 completed only the personality assessment and did not provide qualitative responses. To maintain analytical rigor, participants were divided into two groups based on completion status.

Participants who completed the entire study (Group 1; $n = 196$) were included in all behavioral coding procedures and regression analyses examining the relationships between personality traits and intrusion behaviors. Participants who completed only the personality measures (Group 2; $n = 61$) were retained for descriptive and demographic analyses but excluded from behavioral outcome analyses because they lacked scenario responses.

The differential completion introduces the potential for attrition bias, as individuals who fully completed the study may differ systematically from those who discontinued before the open-ended portion. Participants who persisted in completing the survey may reflect higher engagement, greater interest in cybersecurity scenarios, or greater comfort articulating technical reasoning. As a result, behavioral findings primarily reflect the decision-making patterns of more motivated respondents and may underrepresent individuals with lower task engagement or differing cognitive styles. Although including Group 2 supported broader demographic characterization of the sample, behavioral inferences are necessarily limited to those who completed the full intrusion exercise.

This method enabled the study to make the most of the available data while ensuring consistency between predictors and outcomes. By limiting behavioral analyses to participants who completed the entire protocol, the study prevented bias or missing data from affecting models that relied on both personality measures and behavioral indicators.

For Group 1 (n = 196), participants' ages ranged from 18 to 70 years (M = 36.83, SD = 11.29). The interquartile range showed that 50% of participants were between 29 and 43 years old, with a median age of 35.

In Group 2 (n = 61), participants ranged in age from 19 to 63 years (M = 38.56, SD = 11.82). The interquartile range indicates that 50% of participants were between 28 and 47 years old, with a median age of 37.

Table 9 shows that both groups had similar age distributions, with comparable means, medians, and variability. This suggests that failing to complete the open-ended section was not closely related to age and alleviates concerns that attrition caused systematic demographic bias between the groups.

Table 9.

Age Breakdown by Group

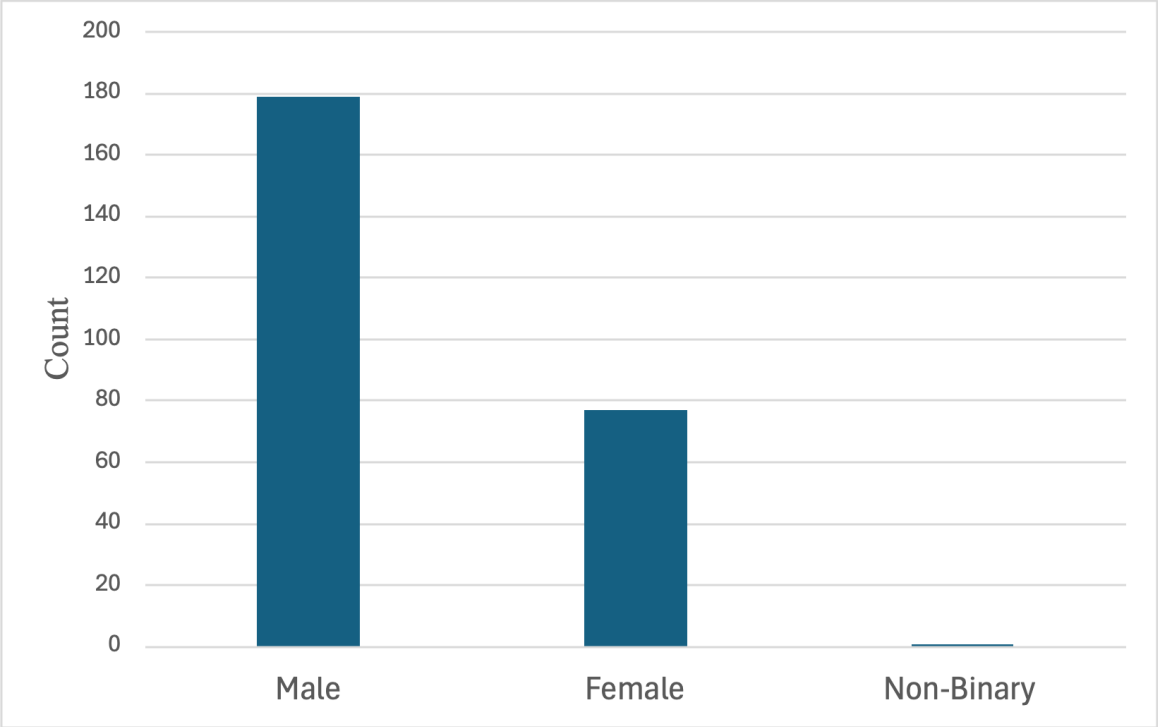
Statistic	Group 1 (n = 196)	Group 2 (n = 61)
Mean	36.83	38.56
SD	11.29	11.82
Minimum	18	19
25th Percentile	29	28
Median	35	37
75th Percentile	43	47
Maximum	70	63

Consistent with prior research on cybersecurity workforce demographics, the sample was predominantly male, with approximately 70% of participants identifying as male, 30% as female,

and one participant identifying as non-binary (Figure 5). Previous studies have similarly documented male overrepresentation in cybersecurity and technical fields (Kennison & Chan-Tin, 2020; Papatsaroucha et al., 2021; Russell et al., 2017). While this distribution reflects industry norms, the limited gender diversity limits the generalizability of the findings and underscores the need for future research that examines more demographically diverse populations.

Figure 5.

Gender Breakdown



The gender imbalance aligns with workforce demographics in the cybersecurity sector, where men constitute most of the workforce (ISC², 2023). Reports indicate that women face barriers to entry and promotion, resulting in their underrepresentation in the field (ISC², 2024).

Both groups were predominantly White or Caucasian respondents in terms of race and ethnicity (Table 10). Although there was some diversity, the predominance of White participants underscores the limited representation of other racial and ethnic groups, highlighting ongoing diversity challenges in the cybersecurity sector.

Table 10.

Race and Ethnicity Breakdown

	Group 1 (*n* = 196)	**Group 2 (*n* = 61)**	**Total (*n* = 257)**	**Group 1 Percent (*n* = 196)**	**Group 2 Percent (*n* = 61)**	**Total Percent (*n* = 257)**
White or Caucasian	115	35	150	58.7%	57.4%	58.4%
Black or African American	37	8	45	18.9%	13.1%	17.5%
American Indian/Native American or Alaska Native	7	1	8	3.6%	1.6%	3.1%
Asian	26	12	38	13.3%	19.7%	14.8%
Native Hawaiian or Other Pacific Islander	1	0	1	0.5%	0%	.4%
Other	5	4	9	2.6%	6.6%	3.5%
Prefer Not to Say	5	1	6	2.6%	1.6%	3.5%
Spanish, Hispanic or Latino Origin	17	5	22	8.7%	8.2%	8.6%
Not Spanish, Hispanic or Latino Origin	179	56	235	91.3%	91.8%	91.4%

Regarding marital status (Table 11), respondents most frequently identified as married, with 'never been married' as the second most common. Although most participants were either married or had never been married, individuals from all categories were represented, indicating a diverse range of relationship statuses in the sample.

Table 11.

Marital Status Breakdown

	Group 1 (*n* = 196)	**Group 2 (*n* = 61)**	**Total (*n* = 257)**	**Group 1 Percent (*n* = 196)**	**Group 2 Percent (*n* = 61)**	**Total Percent (*n* = 257)**
Married	82	27	109	41.8%	44.3%	42.4%
Living with Partner	24	5	29	12.2%	8.2%	11.3%
Widowed	1	17	2	0.5%	1.6%	0.8%
Divorced/Separated	15	21	22	7.7%	11.5%	8.6%
Never Been Married	74	61	95	37.8%	34.4%	37%

As shown in Table 12, participants' educational attainment was notably high. More than half of all participants reported holding a Bachelor’s degree. Group 2 had a slightly greater proportion of individuals with advanced degrees than Group 1. Across the entire sample, fewer participants had only a high school diploma or some college, and no one reported less than a high school education. This indicates that most individuals in the study completed higher education.

Table 12.

Education Breakdown

	Group 1 (*n* = 196)	Group 2 (*n* = 61)	Total (*n* = 257)	Group 1 Percent (*n* = 196)	Group 2 Percent (*n* = 61)	Total Percent (*n* = 257)
Less than High School Degree	0	0	0	0%	0%	0%
High School Graduate	11	1	12	5.6%	1.6%	4.7%
Some College but No Degree	35	11	46	17.9%	18%	17.9%
Associates Degree	16	1	17	8.2%	1.6%	6.6%
Bachelors Degree	98	35	133	50%	57.4%	51.8%
Masters Degree	34	11	45	17.3%	18%	17.5%
Doctoral Degree	2	1	3	1%	1.6%	1.2%
Professional Degree (JD/MD)	0	1	1	0%	1.6%	0.4%

Most participants in the study reported being employed (Table 13). This aligns with the professional culture of the cybersecurity and penetration testing communities where recruitment took place.

Table 13.

Employment Status Breakdown

	Group 1 (*n* = 196)	Group 2 (*n* = 61)	Total (*n* = 257)	Group 1 Percent (*n* = 196)	Group 2 Percent (*n* = 61)	Total Percent (*n* = 257)
Working (Paid Employee)	151	48	199	77%	78.7%	77.4%
Working (Self Employed)	19	2	21	9.7%	3.3%	8.2%
Not Working/Laid Off	4	1	5	2%	1.6%	1.9%
Not Working/Seeking	15	5	20	7.7%	8.2%	7.8%
Not Working/Retired	4	0	4	2%	0%	1.6%
Not Working/Disabled	1	1	2	0.5%	1.6%	0.8%
Not Working/Other	1	4	5	0.5%	6.6%	1.9%
Prefer Not to Say	1	0	1	0.5%	0%	0.4%

As previously noted, the demographics questionnaire was revised to add a question about cybersecurity involvement (Table 14). Participants showed a range of involvement levels, with responses across all categories. System Admin/IT Professionals made up the largest group, followed by hobbyists as the second-largest group. Including these diverse groups broadens the applicability of the findings by reflecting opinions from both beginners and experienced practitioners.

Table 14.

Cybersecurity Involvement Breakdown

	Group 1 (*n* = 196)	Group 2 (*n* = 61)	Total (*n* = 257)	Group 1 Percent (*n* = 196)	Group 2 Percent (*n* = 61)	Total Percent (*n* = 257)
Hobbyist	40	16	56	20.4%	26.2%	21.8%
Student	34	9	43	17.3%	14.8%	16.7%
Aspiring Professional	29	4	33	14.8%	6.6%	12.8%
Penetration Tester	11	3	14	5.6%	4.9%	5.4%
Security Researcher/Bug Bounty Hunter	9	1	10	4.6%	1.6%	3.9%
Security Professional (Leadership/Academia)	10	6	16	5.1%	9.8%	5.4%
System Admin/IT Professional	53	15	68	27%	24.6%	26.5%
Other	10	7	17	5.1%	11.5	6.6%

Scale Reliability and Assumption Checks

Prior to testing the hypotheses, the reliability of the personality assessments and the consistency of qualitative data coding were confirmed. The Big Five Inventory (BFI) and the Short Dark Triad (SD3) scales showed acceptable to strong internal consistency, with Cronbach's α values for the BFI ranging from 0.72 to 0.84 across the five trait dimensions (Table 15), meeting established reliability thresholds in behavioral research ($\alpha \geq 0.70$). These values indicate that the constructs were measured with sufficient consistency for inferential analysis.

Table 15.

Big Five Inventory Cronbach's α

Extraversion	0.72
Agreeableness	0.78
Conscientiousness	0.84
Neuroticism	0.74
Openness	0.80

The SD3 traits varied from 0.70 to 0.82 (see Table 16). These scores surpassed the commonly accepted threshold of 0.70, which signifies sufficient reliability for research purposes (Nunnally & Bernstein, 1994).

Table 16.

Short Dark Triad Cronbach's α

Machiavellianism	0.82
Narcissism	0.76
Psychopathy	0.70

Statistical assumption checks were conducted for the regression models. Scatterplots confirmed linearity between continuous predictors and the logit of the dependent variables. Residuals showed no signs of non-normality. VIF scores were below 2.0 for all predictors, indicating multicollinearity was not problematic. Residual scatterplots demonstrated consistent variance, supporting homoscedasticity. The Durbin-Watson statistic ranged from 1.7 to 2.1, indicating no evidence of autocorrelation.

Qualitative data required interrater reliability to confirm consistent binary coding of open-ended responses. Two coders independently reviewed a 20% subset of responses. Their coding was compared, and Cohen's κ was used to measure agreement. The κ was 0.98, indicating near-perfect agreement per Landis and Koch (1977). This high reliability confirms the trustworthiness of the coded data.

The initial checks confirmed that the data met the essential reliability and assumption standards, providing a reliable basis for the subsequent regression and inferential analyses.

Big Five Tests

The Big Five Inventory used a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) to assess the personality dimensions (Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness). Scores ranged from 1 to 5, showing significant variation among participants. Descriptive statistics for these traits are presented in Appendix D.

Among the 257 participants, Conscientiousness ($M = 3.94$, $SD = 0.69$) and Agreeableness ($M = 3.85$, $SD = 0.63$) were the most prominent traits. This aligns with earlier research showing that people in technical or analytical roles tend to score higher on Conscientiousness, which reflects organization, persistence, and discipline (Dupuis & Gleason, 2020; Fagade et al., 2019; McBride et al., 2018). These traits are associated with structured intrusion strategies.

Openness ($M = 3.78$, $SD = 0.61$) was moderately high, reflecting curiosity, creativity, and intellectual engagement, traits thought to predict the use of innovative and complex intrusion techniques. Conversely, Extraversion ($M = 3.04$, $SD = 0.86$) and Neuroticism ($M = 2.61$, $SD = 0.86$) were lower, consistent with previous research indicating that cybersecurity professionals tend to be introverted and emotionally stable (Dupuis & Gleason, 2020; Fagade et al., 2019; McBride et al., 2018).

The Big Five results indicated that participants primarily showed high Conscientiousness and Agreeableness, with moderate Openness and lower Extraversion and Neuroticism. These findings align with prior research in cybersecurity and technical fields, where such individuals often exhibit higher Conscientiousness and emotional stability (Dupuis & Gleason, 2020; Fagade et al., 2019; McBride et al., 2018). These distributions provide context for subsequent analyses of associations between personality traits and intrusion behaviors.

Dark Triad Tests

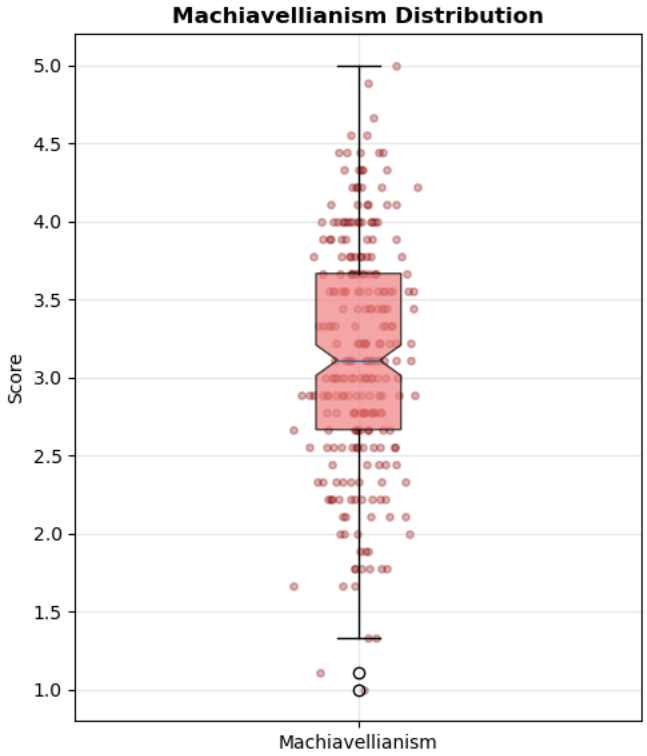
Descriptive statistics (see Appendix D) for the Short Dark Triad (SD3) were examined to investigate participants' dark personality traits. Similar to the Big Five data, statistics were computed for the full sample (n = 257) and for two participant subgroups (Group 1 and Group 2). Each Dark Triad trait (Machiavellianism, Narcissism, and Psychopathy) was examined individually to assess average levels and variability among participants. An overall Dark Triad score was also created by averaging these three traits, providing a general measure of dark personality tendencies. This composite score supported both comprehensive hypothesis testing and detailed examination of each trait's role.

The SD3 traits were evaluated using a 5-point Likert scale, with respondents indicating their level of agreement from 1 (Strongly Disagree) to 5 (Strongly Agree). Scores spanned the full 1-5 range, indicating notable variability among participants. Most scores clustered around the middle, but a smaller subgroup reported very low or very high scores. This distribution reveals significant individual differences in dark personality traits, pointing to a wide range of manipulative, self-centered, or impulsive tendencies.

Across the sample (n = 257), participants reported average scores near the midpoint of the scales. Machiavellianism scored highest (M = 3.14; SD = 0.74), indicating a tendency to endorse behaviors related to manipulation, strategic thinking, and self-interest. As shown in Figure 6, the distribution of Machiavellianism scores was centered on the scale midpoint, with few extreme values, suggesting variability within a generally moderate range rather than elevated or pathological levels.

Figure 6.

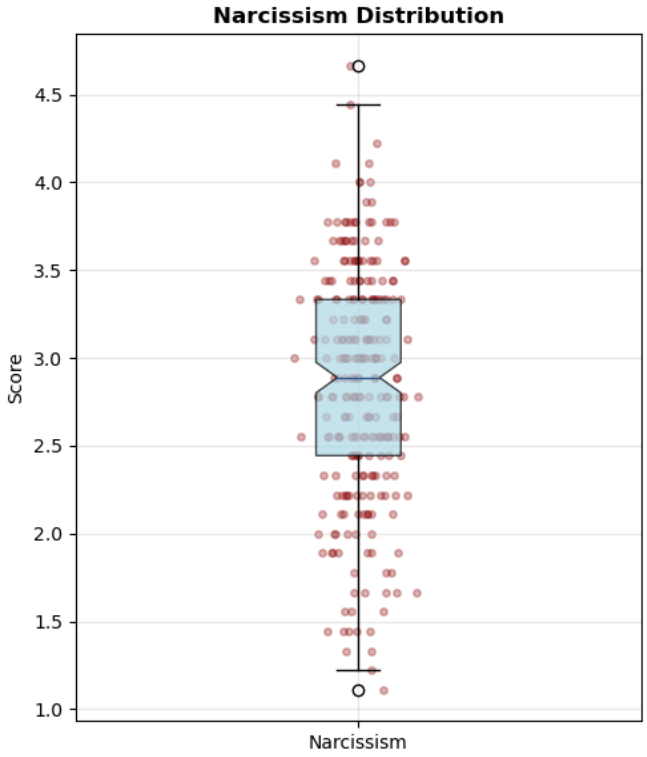
Distribution of Machiavellianism Scores in the Sample (n = 257)



Narcissism scores were near the scale's midpoint ($M = 2.84$; $SD = 0.66$), indicating moderate confidence and self-focus among participants. As shown in Figure 7, the distribution was approximately symmetrical with few outliers, indicating that very high narcissistic traits were rarely endorsed.

Figure 7.

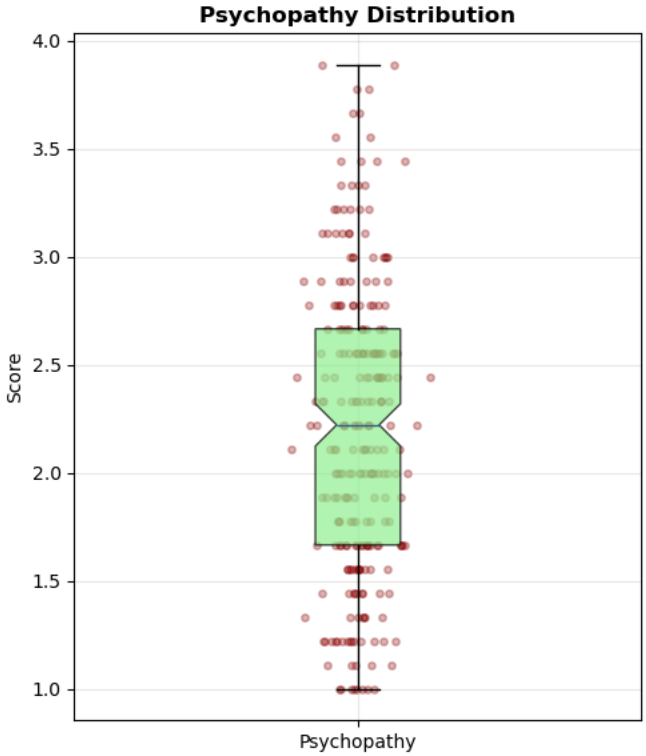
Distribution of Narcissism Scores in the Sample (n = 257)



Psychopathy scores were the lowest among the Dark Triad traits (M = 2.20; SD = 0.68). As shown in Figure 8, the distribution was concentrated below the scale, with most participants reporting low levels of psychopathic traits. Despite some variability, the overall trend suggests limited self-reported impulsivity, callousness, or emotional detachment in the sample.

Figure 8.

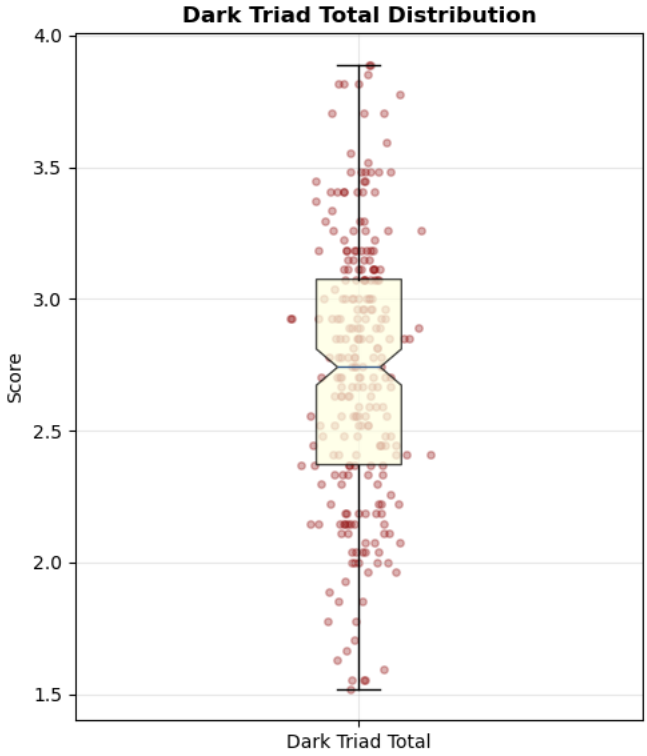
Distribution of Psychopathy Scores in the Sample (n = 257)



An overall Dark Triad score was computed by averaging scores on Machiavellianism, Narcissism, and Psychopathy ($M = 2.73$; $SD = 0.51$; Figure 9). This composite measure was used alongside individual trait scores to capture common variance among the Dark Triad traits and to serve as a broader indicator of darker personality tendencies (Jones & Paulhus, 2014; Paulhus & Williams, 2002). The distribution shows moderate endorsement across the sample, indicating the presence of dark traits without reaching extreme or clinical levels.

Figure 9.

Dark Triad Total Distribution Scores (n = 257)



Overall, the results show that the sample had moderate levels of Machiavellianism and Narcissism and lower levels of Psychopathy. This pattern indicates that participants tended to favor strategic, goal-driven behaviors over traits associated with emotional detachment or impulsivity. These baseline distributions lay the groundwork for further analyses of how differences in Dark Triad traits influence intrusion behavior across the models.

Analytical Framework

Inferential statistics were employed to examine the study's research questions and hypotheses. The analysis focused on how personality traits influence participants' choices in a simulated cyber intrusion scenario. The following sections integrate both quantitative and

qualitative results to provide a comprehensive overview of personality-related cybersecurity behaviors.

To examine the research questions, a series of correlational and regression analyses were conducted. Pearson's correlation coefficients were computed to assess relationships between personality traits and binary-coded intrusion behaviors derived from qualitative responses. Logistic regression and multivariate models were then used to evaluate the predictive power of personality traits while controlling for demographic factors. Additionally, Random Forest classification was used as a supplementary validation technique to enhance the model's robustness and minimize overfitting.

Model fit was assessed with Pseudo R^2 because logistic regression was used to predict binary intrusion behaviors. Unlike linear regression, logistic models do not generate a standard R^2; instead, Pseudo R^2 indices estimate relative explanatory power by comparing the fitted model to a null model without predictors. These values should be seen as indicators of how well the model performs relative to a baseline, rather than precise measures of variance explained.

In applied behavioral and social science research, Pseudo R^2 values of 0.10 to 0.30 are typically interpreted as evidence of significant predictive relationships, particularly when analyzing complex decision-making processes influenced by many interacting factors (Chen et al., 2010). Therefore, the Pseudo R^2 values in this study are viewed as evidence of a meaningful explanatory structure rather than as an exact measure of variance explained.

In addition to quantitative models, qualitative data from open-ended responses were analyzed to provide behavioral and psychological insights into the statistical results. Responses were systematically coded using a tailored codebook based on the MITRE ATT&CK Framework, for psychological analysis. This framework served as the primary taxonomy for

identifying intrusion stages and specific TTPs mentioned in responses. The categories were expanded to include behavioral aspects such as boldness, structure, creativity, and deception. These additions help capture cognitive and motivational factors in decision-making that MITRE ATT&CK's technical focus does not address.

The codebook was refined through an iterative process involving reviews and discussions with industry peers. It was continually compared to MITRE ATT&CK's existing TTP framework to ensure conceptual consistency while maintaining psychological relevance. Responses from each participant were examined and assigned a binary code: zero (0) indicating absence, and one (1) indicating presence for each category. This binary coding method was used to emphasize the presence or absence of specific behaviors rather than how often they were mentioned. Since each open-ended response reflected a distinct phase of the intrusion scenario, the focus was on whether the behavior was expressed rather than on its frequency. This strategy ensured consistent, reproducible scoring, minimized subjectivity, and enabled integration with quantitative models.

The mixed-methods approach connected psychological constructs with technical TTP classification, allowing a thorough interpretation of how personality influences intrusion decision-making. This method helped explain why specific TTPs were selected, showing that real-world intrusion decisions are driven not just by procedural logic but also by underlying personality factors.

The multi-method analytical framework enabled triangulation of statistical and behavioral data. By integrating correlational, regression, and machine-learning techniques with qualitative coding, the study strengthened the validity of its findings both internally and externally. The sequential approach, beginning with quantitative pattern analysis and concluding

with qualitative contextualization, ensured a comprehensive examination of personality-behavior relationships from both structural and interpretive perspectives.

Correlation Analysis

Pearson's correlation analyses were performed to explore the links between personality traits and cyber intrusion behaviors. This step was the first quantitative approach to connect participants' psychological profiles with their behaviors during the tabletop segment. Using binary coding for behaviors (1 = present; 0 = absent), the analysis examined whether certain traits were linearly associated with specific intrusion tactics.

This section begins with zero-order correlations, which represent unadjusted bivariate associations between variables. Following the zero-order correlations is a synthesis of observed correlational patterns. The correlational analyses provide a foundational understanding of the direction and strength of relationships before the multivariate modeling presented in the subsequent sections.

Zero-Order Correlation

Zero-order correlations were computed to examine bivariate relationships between personality traits and cyber intrusion behaviors before multivariate modeling. These correlations reflect unadjusted associations and provide an initial assessment of the direction and strength of relationships, without controlling for demographic factors or overlap among personality dimensions. Table 17 presents the zero-order Pearson correlations. The correlations were computed to examine unadjusted bivariate relationships between personality traits and intrusion behaviors prior to multivariate modeling.

Table 17.

Bivariate (Zero-Order) Correlations Between Personality Traits and Cyber Intrusion Behaviors

Personality Trait	Bold	Deceptive	Creative	Sophisticated	Structured	High-Risk	Aggressive	Persistent	Ransomware
Openness	-0.50	0.012	0.026	-0.058	-0.129*	-0.004	0.078	-0.134*	0.083
Conscientiousness	-0.084	-0.011	-0.106	-0.074	-0.125*	-0.038	-0.047	-0.021	0.050
Extraversion	0.025	-0.063	0.100	0.069	0.081	-0.037	0.010	0.023	0.077
Agreeableness	-0.282**	-0.218**	-0.014	-0.131*	-0.236**	-0.149*	-0.080	-0.091	0.026
Neuroticism	0.085	0.033	-0.091	0.056	0.048	0.072	0.088	0.045	-0.037
Machiavellianism	0.114	0.111	-0.030	0.166**	0.012	0.131*	0.090	0.035	.179**
Narcissism	0.158*	0.022	0.067	0.162**	0.040	0.134*	0.060	0.118	.240**
Psychopathy	0.392**	0.285**	0.244**	0.405**	0.145*	0.168**	0.265**	0.169**	.166**
Dark Triad (Total)	0.308**	0.198**	0.118	0.342**	0.091	0.202**	0.195**	0.147*	.271**

Note. $p < 0.05$. $p < 0.01$.

At the zero-order level, Dark Triad traits, particularly Psychopathy, showed the strongest positive associations with bold, deceptive, aggressive, persistent, and sophisticated behaviors. Agreeableness showed consistent negative correlations with multiple high-risk and aggressive behaviors, suggesting a protective association at the bivariate level. Other Big Five traits showed comparatively weaker and more variable relationships across behavioral categories. These baseline associations provided important context for subsequent analyses of the unique predictive contributions of personality traits.

Correlational Patterns Across Personality Traits

Across the sample, the links between personality traits and intrusion behaviors were generally modest. Although several correlations were statistically significant using two-tailed tests ($p < .05$), most fell below the typical threshold for a moderate effect size. Following established behavioral research guidelines (Cohen, 1988), correlations with $|r| \approx 0.30$ or higher were considered substantively meaningful, whereas smaller associations, for completeness, were reported and interpreted cautiously. As shown in Table 18, distinct patterns of correlations emerged across personality domains, with the Dark Triad traits showing the strongest overall links. Notably, psychopathy showed moderate correlations with various high-risk and aggressive intrusion behaviors.

Table 18.

Correlations Across Traits

Trait	Associated Behaviors	r (range)	Statistical Significance	Direction	Interpretation
Psychopathy	Bold, Deceptive, Sophisticated, Aggressive, Persistent	0.265 – 0.405	Bold (p = 0.000000000072) Deceptive (p = 0.000003429) Sophisticated (p = 0.000000000015) Aggressive (p = 0.000016716) Persistent (p = 0.006615)	Positive	Demonstrates the strongest and most consistent associations with high-risk and intrusive behaviors, suggesting a central role in boldness, persistence, and disregard for consequences.
Dark Triad (Total)	Bold, Sophisticated, High-Risk, Aggressive	0.195 – 0.342	Bold (p = 0.000000474) Sophisticated (p = 0.000000018) High-Risk (p = 0.001129) Aggressive (p = 0.001683)	Positive	Demonstrates broad alignment with elevated intrusion risk, reflecting shared variance among maladaptive personality traits.
Agreeableness	Bold, Deceptive, Structured, High-Risk	-.149 – -0.282	Bold (p = 0.000004384) Deceptive (p = 0.000431) Structured (p = 0.000134) High-Risk (p = 0.016832)	Negative	Exhibits consistent negative associations, indicating a protective pattern against aggressive and high-risk intrusion behaviors.
Narcissism	Sophisticated, Ransomware	0.162 – 0.240	Sophisticated (p = 0.009279) Ransomware (p = 0.000102)	Positive	Associated with behaviors involving visibility and perceived mastery, consistent with ego-reinforcing motivations.
Machiavellianism	Sophisticated, High-Risk, Ransomware	0.131 – 0.179	Sophisticated (p = 0.007659) High-Risk (p = 0.035825) Ransomware (p = 0.003991)	Positive	Reflects strategic and outcome-oriented intrusion tendencies, though effects are smaller than Psychopathy.
Big Five (Other Traits)	Variable / Inconsistent	< -0.30	Not significant	Mixed	Openness, Conscientiousness, Extraversion, and Neuroticism demonstrate weaker and less consistent relationships across intrusion behaviors.

Note: Pearson zero-order correlations are reported. Significance tests are two-tailed. p < .05. p < .01.

Psychopathy was less prevalent in the sample; however, it showed the strongest and most consistent associations with intrusion behaviors across all personality traits examined. Psychopathy exhibited moderate positive correlations with bold, deceptive, sophisticated, aggressive, and persistent behaviors. Several associations met or exceeded conventional thresholds for moderate effect size ($|r| \approx 0.30$). These patterns indicate that those higher in Psychopathy are more likely to engage in intrusion behaviors characterized by persistence, risk tolerance, and reduced concern for detection or consequences. Although these findings are correlational and should be interpreted cautiously, they align with the theoretical characterization of Psychopathy as involving impulsivity, low fear sensitivity, and emotional detachment in decision-making contexts.

Beyond Psychopathy, the strongest correlations in the study were with other traits in the Dark Triad. This suggests that maladaptive personality traits are more consistently linked to intrusive behaviors than normal personality dimensions. Specifically, Narcissism and Machiavellianism were positively related to ransomware-related activities. This implies that these traits are associated with intrusion behaviors perceived as impactful and visible. The results align with previous research linking dark personality traits to outcome-focused and power-driven cyber activities (Curtis et al., 2018; Jones et al., 2021).

Machiavellianism was also linked to high-risk intrusion behaviors. These tactics increased the likelihood of detection or exposure, such as targeting high-profile figures or conducting overt reconnaissance. Such patterns imply that individuals with higher Machiavellian traits might be more willing to accept operational risks to achieve strategic or impactful goals. While the connections were moderate, the consistent relationships across different behaviors highlighted the importance of Machiavellianism in intrusion decision processes.

The Big Five personality traits showed distinct yet less uniform associations with intrusion behaviors. Openness was negatively correlated with structured intrusion approaches, suggesting a preference for flexible or unconventional methods over rigid procedures. Conscientiousness was positively associated with reconnaissance activities, indicating that more conscientious individuals tend to favor systematic information collection before proceeding with intrusions. These findings align with prior research linking Openness to adaptability and creativity, and Conscientiousness to organized, goal-driven cyber activities (Fagade et al., 2017; Matulessy & Humaira, 2016; Shappie et al., 2019).

The majority of observed correlations were small in magnitude, consistent with prior cybersecurity personality research showing that individual personality traits explain only a limited proportion of variance in cyber intrusion and deviant behavior (Curtis et al., 2018; Harms et al., 2022; Jones et al., 2021). Taken together, these correlational patterns provide a foundational context for subsequent regression analyses that assess the unique predictive contributions of personality traits while accounting for overlap among predictors.

Regression Analysis

Regression analyses were conducted to examine the predictive relationships among the Big Five and Dark Triad personality traits and participants' cyber intrusion behaviors. The primary goal was to determine whether personality factors could reliably predict the behaviors selected during a simulated cyber intrusion. Outcome variables included boldness, structure, and persistence.

An alpha level of $p < 0.05$ was used to assess statistical significance. Odds ratios (ORs) were reported with corresponding 95% confidence intervals (CIs). ORs greater than 1 indicated a

higher likelihood of engaging in a specific behavior, whereas ORs less than 1 indicated a lower likelihood.

While statistical significance indicates whether an observed relationship is unlikely to be due to chance, odds ratios help assess its strength. In behavioral and social science research, odds ratios between 1.3 and 1.7 typically indicate meaningful effects, especially in complex decision-making involving multiple interacting factors (Chen et al., 2010). Therefore, in this study, odds ratios are interpreted as indicators of physical-behavioral influence rather than precise predictions.

The analyses were carried out in three sequential steps. First, binary logistic regression was used to assess how well each personality trait could directly predict individuals' intrusion behaviors. Second, a moderation model tested whether age influenced the relationship between psychopathy and behavioral tendencies. Finally, multivariate logistic regression models combining all the demographic factors evaluated their combined effect.

The systematic approach went beyond basic correlations by examining both the direction and the strength of each effect. This provided a clearer understanding of how personality traits interact with other factors to influence decisions about cyber intrusions.

Binary Logistic Regression

Binary logistic regression analyses were performed to evaluate whether traits from the Big Five and Dark Triad models could predict the likelihood of cyber intrusion behaviors. Each behavior was considered a binary variable, coded as one (1) for presence and zero (0) for absence in the open-ended responses.

The model's accuracy ranged from 58% to 70%, with Pseudo R^2 values from 0.012 to 0.033. This indicates modest explanatory power, suggesting that although personality traits help

predict behavior, they account for only a small share of the total variance. This aligns with expectations for psychological data in complex behavioral contexts.

Among all the predictors, Psychopathy was the only variable that was statistically significant in predicting persistent behavior (OR = 1.40, $p = 0.041$). This indicates that individuals with higher levels of Psychopathy had roughly 40% higher odds of exhibiting persistent behavior in cyber intrusions than those with lower levels.

There were also several directional trends with moderate effect sizes. Dark Triad traits tended to show stronger associations with intrusion behaviors than Big Five traits. The evidence from the models indicates that, while personality alone does not fully predict cyber intrusion behavior, various dimensions, especially psychopathy, serve as meaningful psychological markers of intrusion patterns.

To clearly demonstrate how individual traits influence specific intrusion behaviors, each behavior was examined separately. The following sections highlight key patterns and trends observed in the study.

Reconnaissance

Conscientiousness was not a statistically significant predictor of reconnaissance behavior (OR = 1.49, $p = 0.060$); however, the observed pattern suggested that higher levels of Conscientiousness might be associated with a greater likelihood of engaging in structured information-gathering activities. Although this relationship did not reach traditional significance levels, it indicates a trend that should be interpreted cautiously rather than as a definitive finding.

Qualitative responses provided contextual support for the observed pattern. Several participants described methodical reconnaissance approaches, emphasizing the systematic collection of publicly available information before initiating technical actions. For example, one

participant noted the value of reviewing job postings to infer organizational technologies. At the same time, another described gathering employee names, email formats, and other details from LinkedIn, corporate websites, and other publicly available, search-indexed open-source sources to guide Social Engineering efforts.

- "You can do some additional information gathering by looking at any job postings they have and seeing what skills they are looking for. This will give you some insight into what software and technologies they are using."
- "You can use LinkedIn and social media to gather names of employees who work there to stage some Social Engineering attacks."
- "would gather public info like staff names, emails, and tech used. Look through LinkedIn, websites, and search tools."

The narratives demonstrate careful planning and thoroughness, aligning with Conscientious behaviors. While Conscientiousness was not a statistically significant predictor, qualitative evidence suggests that individuals who emphasize organization and preparation may prefer deliberate reconnaissance strategies during the early stages of intrusion.

Social Engineering

In the binary logistic regression model, no predictors were statistically significant for Social Engineering at $p < 0.05$, but notable trends emerged. Extraversion (OR = 1.42, $p = 0.081$) showed a positive association, whereas Agreeableness showed a negative trend (OR = 0.73, $p = 0.092$) with Social Engineering behaviors.

Qualitative responses from the tabletop exercise further reinforced the quantitative patterns. Several participants described selecting strategies that involved interacting with or deceiving employees to gain access.

- "I'd call the helpdesk pretending to be a doctor who lost login credentials."
- "Phishing is easier than hacking. People will give you what you need if you sound confident."
- "Social Engineering gets faster results than technical."

The statements demonstrate how participants with higher social skills and confidence used interpersonal relationships to bypass security barriers. Although Social Engineering did not produce statistically significant predictors, the observed relationship and qualitative data indicate that Extraversion and low Agreeableness are key dispositional traits.

Privilege Escalation

Psychopathy showed a positive but non-significant correlation with privilege escalation (OR = 1.34, $p = 0.110$). This pattern suggests that individuals with higher psychopathic tendencies may be more likely to seek elevated system access.

Several responses reflected this cognitive pattern, emphasizing control of the network. One participant stated that the main focus was to gain control of a high-value asset, saying, "control is everything once you are in." Another participant said they would focus on admin rights to remain undetected longer. These statements illustrate a mindset of control and autonomy.

Although privilege escalation was not statistically significant, the pattern suggested that Psychopathy's influence is indirect, promoting bold and persistent tendencies. The identified dominance may manifest across multiple intrusion phases rather than in a single tactic.

Lateral Movement

Two traits approached statistical significance in relation to lateral movement: low Agreeableness (OR = 0.70, $p = 0.062$) and high Openness (OR = 1.37, $p = 0.078$). The negative association with Agreeableness suggests that individuals who are less cooperative, more competitive, and less empathetic may be more inclined to pursue lateral expansion.

Conversely, the positive link with Openness suggests that curious participants who enjoy exploring and are cognitively flexible may be more inclined to try new or unconventional methods to expand network access. This trend appeared in several open-ended responses, with participants describing innovative or unexpected techniques. For example, one participant said they would "pivot through less obvious systems to see where the network leads," while another mentioned they might "try a new vector like IoT devices or printers. Something nobody expects." Others discussed experimenting with "nonstandard ports or unusual access points to see what is possible."

Although these results did not reach conventional statistical significance, they collectively suggest that lateral movement behaviors might be influenced by a combination of competitive motivation (low Agreeableness) and intellectual curiosity (high Openness). This profile aligns with attackers who are technically proficient and adaptable (Paulhus & Williams, 2002).

Evasive Behavior

The results showed that none of the Big Five or Dark Triad traits were statistically significant predictors of evasive behavior. However, several dimensions showed weak directional trends. This suggests that there may be underlying psychological influences on stealthy decision-making, even if they are not statistically significant.

Persistent Behavior

Among all traits examined, Psychopathy was the only significant predictor with persistent behaviors (OR = 1.40, $p = 0.041$). This odds ratio indicates that for each unit increase in Psychopathy, participants were approximately 40% more likely to engage in persistent intrusion behaviors.

Qualitative responses from participants exhibiting persistent behavior reflected this pattern. They often described repeated attempts, changing strategies after failure, and continuing despite obstacles. Examples include statements such as “try again with a different method until something hits” or “keep probing even if the firewall flags it.” These excerpts demonstrate how persistence was expressed behaviorally in the scenario and support the quantitative findings.

Bold Behaviors

Binary logistic regression indicated that Extraversion was positively associated with bold intrusion behaviors (OR = 1.63, $p = 0.0251$), whereas Agreeableness was negatively associated (OR = 0.37, $p = 0.00007$). This suggests that more extraverted individuals are more likely to endorse bold intrusion strategies, whereas those higher in Agreeableness are less likely to do so.

Structured

In the binary logistic regression model, structured behaviors emerged as the strongest overall predictor among the behaviors studied. Two personality traits were statistically significant predictors: Extraversion (OR = 2.39, $p < 0.05$) and Agreeableness (OR = 0.37, $p < 0.05$). Cybersecurity involvement was positively associated with structured behavior, though the association was non-significant.

Multivariate Logistic Regression Models

To extend the analysis beyond single predictors, multivariate logistic regression models were used to assess the influence of personality traits on cyber intrusion behaviors. The models included all personality variables from the Big Five and Dark Triad frameworks, along with moderators such as age, education, cybersecurity involvement, employment, and gender. This approach enabled the examination of both individual and combined effects of psychological and situational factors on cyber intrusion decision-making.

Pseudo R^2 was used to assess the model's performance, providing indicators of predictive reliability and explanatory strength. The values ranged from 0.15 to 0.30, indicating moderate explanatory power. The accuracy ranged from 73% to 96%, suggesting strong predictive reliability. Across all models, Extraversion, Agreeableness, Machiavellianism, and Psychopathy consistently emerged as the most influential predictors. Cybersecurity involvement frequently contributed to higher accuracy, reflecting the role of domain expertise in shaping decision-making patterns.

The multivariate models provided a detailed view of decision-making in cyber intrusion. By considering multiple influences simultaneously, the results explain how personality traits and contextual factors shape behavioral patterns. The following subsections describe the strongest and most interpretable models, highlighting behaviors with the clearest predictive signals.

Structured

Structured behaviors showed the strongest performance among all models, with a Pseudo R^2 of 0.30 and an Accuracy of 92% in the multivariate model. The behaviors indicate an analytical and process-focused approach to intrusions.

The regression model for structured behavior showed the strongest overall fit, underscoring the consistency and interpretability of the behavioral pattern. Personality traits and experience both played meaningful roles in predicting structured approaches, suggesting that organized intrusion decision-making stems from a blend of dispositional tendencies and technical expertise.

Two personality traits emerged as statistically significant predictors: Extraversion and Agreeableness. Extraversion's positive association with structured behaviors (OR = 2.39, p = 0.0027) indicated that those who are more outgoing, assertive, and energetic are over twice as likely to organize their intrusion strategies systematically. Education (p = 0.0166), gender (p = 0.01382), and employment status (p = 0.0174) also demonstrated significant effects.

Agreeableness (OR = 0.37, p = 0.0014) was negatively associated with structured behaviors. This suggests that participants with lower levels of cooperativeness and compliance are more likely to adopt controlled, process-driven approaches.

Cybersecurity involvement also showed a positive directional effect. This suggests that individuals with more professional experience are more likely to use systematic approaches during intrusion attempts. This pattern underscores the importance of domain-specific expertise in promoting structured thinking and adherence to established procedures.

Creative

Creative behaviors demonstrated strong explanatory power with a Pseudo R^2 of 0.28 and a classification accuracy of 95.7%. Significant predictors included Openness (positive), Extraversion (positive), and Education (negative).

Although not statistically significant, a few respondents mentioned they would choose in-person approaches. One participant said they would wear a disguise and walk around the facility,

while another said they would walk slowly as if lost. The findings on creative behavior indicate that individuals who are open-minded, socially confident, and less constrained by formal education are more likely to choose unique and innovative tactics. These respondents exhibited cognitive flexibility and curiosity, traits characteristic of exploratory and inventive cyber intrusions.

Bold

Bold behaviors showed a moderate explanatory power (Pseudo $R^2 = 0.25$) with an overall classification accuracy of 86% in the regression model. Significant predictors included Extraversion (positive), Agreeableness (negative), and age (negative).

Participants with higher levels of Extraversion (OR = 1.63, $p < 0.05$) were significantly more likely to use bold intrusion tactics. Low Agreeableness (OR = 0.37, $p < 0.05$) also predicted the likelihood of choosing bold tactics. Age showed a negative correlation with boldness, indicating that younger people are more likely to choose overt, highly visible tactics than older individuals.

Deceptive

Deceptive behaviors showed a moderate explanatory power (Pseudo $R^2 = 0.25$), with a classification accuracy of 75%. Key predictors included Machiavellianism (positive) and low Agreeableness (negative). Psychopathy had a positive but non-significant trend.

Participants with high Machiavellianism were more likely to use deceptive tactics, such as impersonation and credential abuse. Several high-Machiavellian participants reported tactics that support deception to gain control.

- “Making friends with staff so that I can share a link or email with them. Phishing has a low success rate. Social Engineering is much more productive.”
- “I'd probably social engineer the hospital staff under the guise of being from the IT department and put software on the computers (or trick the employees into putting it on their own computers) that phones home to a C&C server, allowing me to access the machines and their data whenever I want.”
- “Pretend to be an overworked hospital employee.”

Sophisticated

Sophisticated demonstrated moderate explanatory power (Pseudo $R^2 = 0.17$; Accuracy = 91%). The strongest predictors were Conscientiousness (positive), cybersecurity involvement (positive), and a weak but consistent trend for Psychopathy (positive, non-significant).

The positive link with Conscientiousness indicates that individuals who are organized, methodical, and tend to plan are more likely to carry out technically complex or multi-stage attacks.

One participant provided a detailed, multi-phase intrusion strategy that emphasized methodical reconnaissance, human-centric exploitation, and stealth. The response described starting with passive information-gathering, such as collecting data from websites, job postings, and social media. Following that, the participant stated that they would use Social Engineering, perimeter mapping, and selective probing of remote access and vendor portals. The participant explicitly prioritized remaining undetected, avoiding operational disruption, and adapting tactics based on observed defenses, including potential weaknesses in the Managed Security Service Provider (MSSP) monitoring.

Overall, the response demonstrated a highly organized, reconnaissance-led, and ethically guided intrusion strategy, emphasizing persistence, control, and strategic manipulation over direct disruption. Refer to Appendix F for the full response.

Lateral Movement

The multivariate logistic regression model identified both Agreeableness and Openness as significant predictors of lateral movement behavior. Lower Agreeableness was associated with a higher likelihood of lateral movement (OR = 0.45, $p = 0.023$), indicating that individuals who were less cooperative and more competitive were more inclined to expand across networks.

Higher Openness also significantly increased the odds of lateral movement (OR = 2.02, $p = 0.023$), suggesting that individuals with greater cognitive flexibility and exploratory tendencies were more likely to pursue unconventional or adaptive methods to extend access within environments.

High-Risk

The high-risk behavior model showed moderate predictive power (Pseudo $R^2 = 0.23$; Accuracy = 74%), with Machiavellianism (positive) and age (negative) as key predictors. This suggests that strategic manipulation and younger age are associated with greater tolerance for operational risks in cyber intrusion decisions.

This was demonstrated in the statement from participants, such as:

- "Create decoy traffic (e.g., initiate small file transfers from compromised machines to cloud services to create noise)."
- "Hammer EDR it with external alerts."
- "Move to mass destruction."

- "This would be an easy physical recon since the hospital is overwhelmed. I can piggyback and locate high-value systems and employees."

Age showed a negative link to high-risk behaviors. Younger participants, especially those with higher Machiavellianism, were more likely to choose tactics that were noticeable or visible compared to older participants. This pattern suggests that experience, self-regulation, and awareness of potential consequences may reduce high-risk tendencies over time.

Overall, the model indicates that high-risk cyber intrusion behaviors are driven by a combination of strategic thinking and decreased behavioral inhibition. The connection between manipulative intent and youthful assertiveness reflects an archetype of a calculated high-risk taker.

Persistence

The persistence model demonstrated moderate explanatory power (Pseudo $R^2 = 0.21$; Accuracy = 73%). Psychopathy emerged as the primary predictor of persistent intrusion behavior (OR = 1.40, $p = 0.041$), indicating that individuals higher in psychopathic traits were approximately 40% more likely to continue attack attempts despite deterrence or detection.

Although Neuroticism showed a positive bivariate correlation with persistence, it was not a significant predictor once Dark Triad traits were included in the regression model. This suggests that emotional reactivity alone may not significantly influence persistence, whereas fearlessness and goal fixation, key aspects of Psychopathy, are more central to maintaining intrusion behaviors.

The following quotations are direct excerpts from participant responses, illustrating persistent related behaviors:

- "Embedding backdoors within genuine system components like scheduled tasks, Windows services, or Windows Management Instrumentation (WMI)."
- "I will create a firewall so that no one can access my files, and then I will use a vpn so that it is a private connection to the internet."
- "We evade and move to another access point and then log in or switch credentials, so it looks like a new person is breaching in."
- "I will maintain persistence by using fileless techniques like WMI event subscriptions and scheduled tasks that execute obfuscated PowerShell, while avoiding detection by operating during normal work hours and blending in with typical user behavior."

Neuroticism also showed a positive correlation with persistence.

- "I would not stop after being blocked. I would move laterally or change IPs."
- "Even if detected, I would find another way around."

Other Behaviors

The remaining models, which analyzed aggressive, ransomware, and reconnaissance, offered interesting insights; however, they had limited explanatory power (Pseudo $R^2 = 0.15–0.22$; Accuracy = 74–84%). Despite this modest predictive ability, the study provided valuable insights into how personal experiences influence the choice of intrusion tactics.

The model (Pseudo $R^2 = 0.17$; Accuracy = 84%) identified Neuroticism (positive) and Agreeableness (negative) as the primary predictors for aggressive tactics. Statements such as "We run and gun!" and "If you can shut down power, you can disrupt all major functions" reflect a willingness to escalate and assert control through overt damage-causing behaviors.

The ransomware model (Pseudo $R^2 = 0.15$; Accuracy = 84%) identified Narcissism and cybersecurity involvement as positive predictors. The results indicated that confidence and technical skills affect the likelihood of choosing to use ransomware.

Reconnaissance behavior (Pseudo $R^2 = 0.22$; Accuracy = 74%) provided an alternative to overt tactics. Conscientiousness emerged as the most significant positive predictor. Participants with high Conscientiousness were more inclined to undertake systematic data collection prior to attacking. For instance, one participant noted, "I would start by mapping every open port and service before touching anything." This exemplifies the careful and disciplined approach characteristic of reconnaissance.

The models identified different psychological bases for intrusion behaviors. Aggressive actions stem from emotional responses and a need for dominance. Concerns about status and control drive ransomware. Reconnaissance consists of organized, systematic activities conducted before an attack. While the predictive power was only moderate, these findings suggest that cyber intrusions are not merely technical problems but also reflections of personality. Different personality types may lead to distinct operational approaches.

Cross-Model Integration

Cross-model integration was performed to combine results from all multivariate logistic regression models, aiming to uncover common patterns and shared mechanisms underlying intrusion behaviors. This approach enabled a comprehensive review of the behaviors rather than analyzing them separately. It brought together personality traits, demographic data, and contextual factors to collectively explain the observed behavioral outcomes.

Across the multivariate models, personality traits and demographic variables demonstrated significant predictive power. Model performance ranged from moderate to strong

(Pseudo R^2 = 0.15 – 0.30; Accuracy = 73 – 96%), indicating that personality meaningfully contributes to behavioral variance in cyber intrusion scenarios. These performance ranges are summarized across models in Figure 10.

Figure 10.

Dark Triad Odds Ratios By Behavior

	Machiavellianism	Narcissism	Psychopathy
Aggressive	1.326	1.240	2.423
Evasive	1.394	1.226	1.704
Lateral Movement	0.996	1.153	1.259
Persistent	1.098	1.450	1.633
Privilege Escalation	1.292	1.313	1.630
Ransomware	1.820	2.607	1.750
Reconnaissance	0.952	1.095	1.189
Social Engineering	1.525	1.006	1.118

Structured, creative, and bold models proved to be the most effective overall predictors of behavioral differences. The structured model (Pseudo R^2 = 0.30, Accuracy = 92%) was marked by higher Extraversion, lower Agreeableness, and increased involvement in cybersecurity, suggesting that socially assertive and technically experienced individuals generally favor organized and methodical approaches.

Creative (Pseudo R^2 = 0.28, Accuracy = 96%) was primarily associated with higher Openness and Extraversion, suggesting that cognitive flexibility and confidence are linked to innovative and exploratory intrusion strategies. Bold (Pseudo R^2 = 0.25, Accuracy = 86%) was more strongly associated with younger participants and lower empathy, reflecting a greater propensity for risk-taking and stimulation-seeking behaviors.

The Dark Triad traits, particularly Psychopathy and Machiavellianism, consistently predicted persistence, deception, and high-risk behaviors across models. In the binary logistic

regression model for persistence, Psychopathy was the only trait to reach statistical significance (Persistence OR = 1.40, $p = 0.041$), indicating a higher likelihood of continued intrusion attempts when deterrence was encountered.

In contrast, multivariate models and cross-model analyses revealed stronger, more consistent directional effects of Psychopathy across multiple intrusion behaviors, including persistence, evasion, and complex operations. Although these effects did not always reach statistical significance across multivariate models, their consistency across behaviors suggests a stable association between Psychopathy traits and sustained, goal-oriented intrusion strategies. Qualitative responses reinforced this pattern, with participants reporting that they "keep probing even if detected" or "move laterally if blocked," reflecting persistence and reduced sensitivity to deterrence.

Machiavellianism was positively associated with deception and risk-taking, supporting the interpretation of calculated, manipulative behavior aimed at gaining control or an advantage. Several respondents described posing as employees or contractors to gain access, or intentionally forming relations to deceive targets. These behaviors reflect deliberate, strategic manipulation, consistent with Machiavellian tendencies.

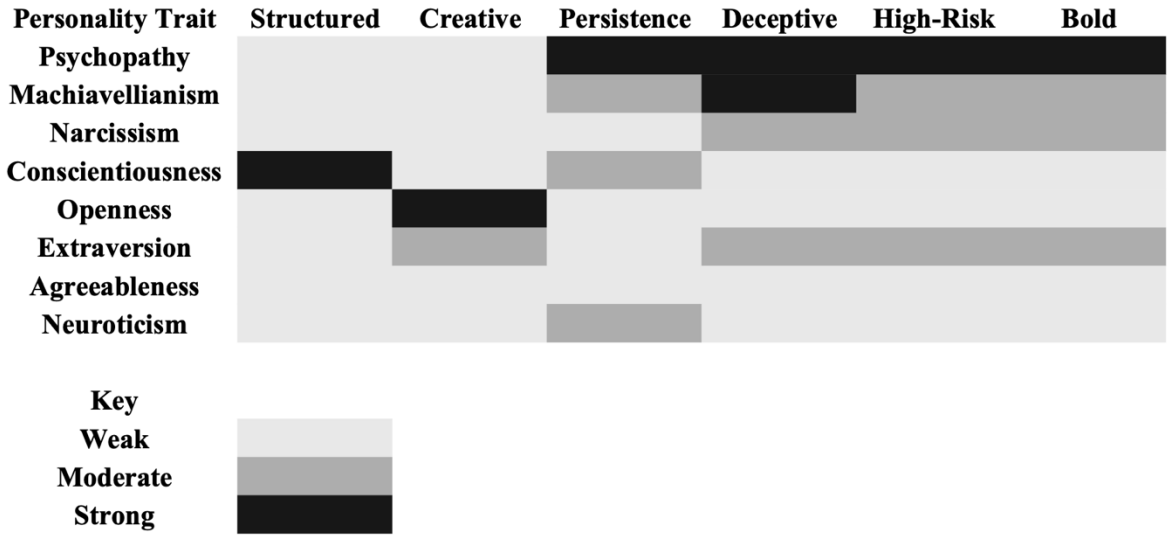
Among the Big Five traits, Openness and Conscientiousness showed the most consistent effects across models. Participants high in Openness frequently demonstrated cognitive flexibility, saying they would "try something unconventional, like rerouting through a different server" or "improvise when a plan fails." In contrast, higher Conscientiousness was associated with structured, methodical reasoning, emphasizing planning, documentation, and systematic reconnaissance. Together, these traits illustrate that normative personality dimensions shape intrusion style rather than intent.

Demographic factors also significantly influenced ithechoices of intrusion. Age was consistently associated with lower engagement in bold, high-risk behaviors, indicating that impulsivity tends to decline with age. Conversely, cybersecurity involvement strengthened predictive performance across multiple models, including those for structured, sophisticated, and ransomware behaviors, suggesting that technical experience amplifies personality-driven decision-making.

A synthesis of multivariate results suggests an integrated pattern of personality influences on cyber intrusion decision-making within the present sample. Dark Triad traits were consistently associated with manipulative, high-risk, and persistent behavioral tendencies. In contrast, Big Five traits were more strongly related to cognitive style and structures, as well as to creative approaches to intrusions. As illustrated in Figure 11, Dark Triad traits showed stronger and more consistent associations with persistence, deception, high-risk and bold behaviors, whereas Big Five traits were more prominently linked to structured and creative intrusion styles.

Figure 11.

Cross-Model Heatmap of Personality Traits and Intrusion Behaviors



The pattern observed in cross-model integration supports the study's main idea that intrusion behaviors stem from both personality and situational factors. The results show that an attacker's decisions can be accurately modeled using their unique psychological profile and experimental variables. This approach can predict not only whether they will act but also how they will strategize, adapt, and persist, thereby indicating the potential extent of damage they could cause to a network.

Moderation Analysis

To examine whether demographic factors influence the relationship between personality traits and intrusion behaviors, moderation analyses were conducted. Age was selected as the primary moderator of interest, based on previous research indicating that Psychopathy and risk tendencies decline with age and maturity (Hare, 2003). Additional exploratory analyses were

conducted for other demographic variables, including ethnicity and marital status, to assess whether cultural or contextual factors affect these relationships.

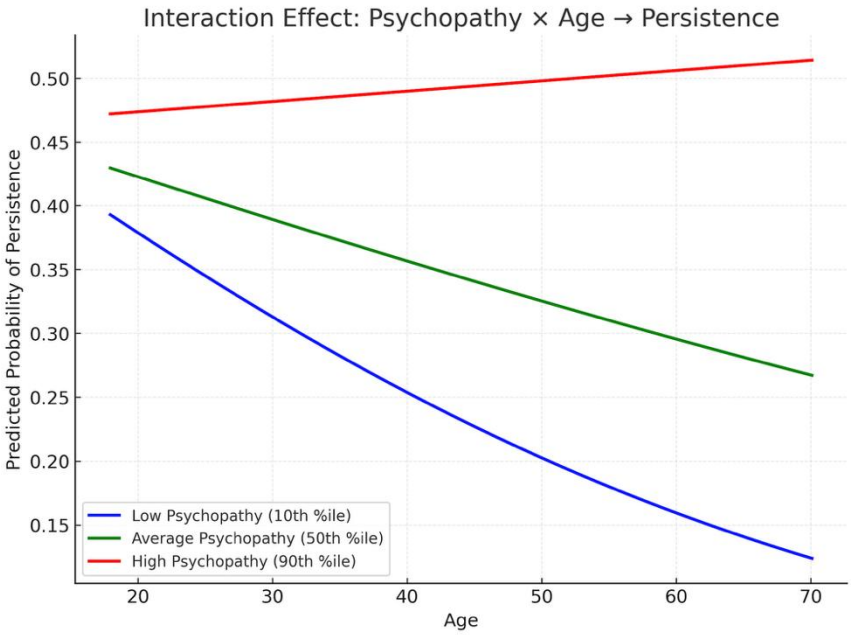
The analyses extended binary logistic regression models by examining interactions among Dark Triad traits, demographic variables, and intrusion behaviors. Predictors were standardized before analysis to improve interpretation and reduce multicollinearity.

Age and Psychopathy

The moderation analysis revealed a notable interaction between Psychopathy and age in forecasting persistent intrusion behavior. As shown in Figure 12, persistence decreased with age in individuals with low and moderate Psychopathy, with the most pronounced decline in the low-Psychopathy group. Conversely, those with high Psychopathy maintained relatively consistent levels of persistence across different ages. This suggests that elevated Psychopathy lessens the typical age-related decrease in persistence, implying that psychopathic traits might shield against the inhibitory influence of aging on ongoing intrusion behavior.

Figure 12.

Psychopathy x Age Interaction Effect on Persistence



Age, Machiavellianism, and Narcissism

While Psychopathy showed an interesting moderating effect, Machiavellianism and Narcissism exhibited a more consistent behavioral pattern across age.

Machiavellianism and age interact subtly yet meaningfully with persistence. In younger individuals, Machiavellianism was less likely to predict persistence after detection or failure. However, in older individuals, higher levels of Machiavellianism predicted greater persistence over time. This suggests that as people age, their strategic manipulation and long-term planning skills improve, aligning more with calculated persistence than with impulsive risk-taking. Although this trend did not reach the conventional statistical significance threshold of $p < 0.05$, the widening gap in predicted probabilities across age points suggests a shift in how Machiavellianism manifests behaviorally over time.

In contrast, Narcissism and age showed a consistent positive relationship with persistence across all age groups. Similar slopes were observed among younger and older participants. This stability indicates that narcissistic motivations, such as the desire for recognition, control, and validation, remain relatively constant throughout adulthood.

Other Moderators

While age was the primary factor influencing interest, exploratory analyses were also conducted to assess whether other demographic variables, such as ethnicity or marital status, moderated the relationship between personality traits and intrusion behaviors. Although these effects were not hypothesized in advance, two notable interaction patterns emerged.

Ethnicity showed a moderate interaction with high-risk behaviors, with an interaction magnitude of 1.42. Participants identifying with underrepresented ethnic groups had slightly higher predicted probabilities of engaging in high-risk intrusion methods. However, the sample sizes across groups were unevenly distributed; therefore, this finding should be viewed as exploratory and interpreted with caution.

Marital status also interacted with high-risk behavior (interaction magnitude of 1.05). Single participants showed marginally higher predicted probabilities of choosing riskier intrusion strategies than married participants. This may reflect differences in risk tolerance or time investment.

Random Forest Validation

Multiple analytical approaches were intentionally employed to examine the personality-behavior relationships from complementary perspectives. Zero-order correlations were used to identify initial associations between traits and intrusion behaviors. Binary logistic regression

models were then applied to test predictive effects while controlling for demographic variables and overlapping personality traits. Finally, a random forest classifier was implemented as a validation technique to assess the robustness of these relationships, capture potential non-linear interactions, and evaluate the model's performance in a data-driven manner. Together, these methods provided convergent evidence and reduced reliance on any single statistical approach.

To complement traditional statistical analyses and evaluate the robustness of predictive relationships between personality traits and intrusion behaviors, a Random Forest validation model was employed. This approach was selected for its ability to capture complex, nonlinear interactions among predictors that conventional regression models may overlook, as well as its effectiveness in ranking variable importance (Breiman, 2001). Whereas regression models identify directional effects and statistical significance, Random Forest offers an additional perspective by assessing predictive accuracy through ensemble learning and internal cross-validation (Breiman, 2001). Within this mixed-methods framework, machine learning provided a quantitative mechanism for validating behavioral patterns derived from qualitative coding. Table 19 presents the key predictors identified through the Random Forest validation and their alignment with regression findings.

Table 19.

Random Forest Validation: Key Predictor Importance

Predictor	Mean Importance Score	Rank	Behaviors Influenced
Psychopathy	0.41	1	Persistence, Bold, High-Risk
Machiavellianism	0.28	2	Deception, High-Risk
Conscientiousness	0.24	3	Structured, Sophisticated
Extraversion	0.19	4	Creative
Narcissism	0.17	5	Ransomware, Impact
Age	0.12	6	Persistence
Cybersecurity Involvement	0.11	7	Sophisticated
Education	0.10	8	Structured

The inclusion of a machine learning validation phase aimed to verify if the patterns observed in the regression models were consistent and to assess whether the variables could reliably forecast behavioral outcomes beyond chance. This step improved the mixed-methods approach by combining the quantitative findings from the regression with predictive modeling, offering a thorough evaluation of the link between personality and behavior in cyber intrusions.

The Random Forest model was trained on the subset of participants who completed the full study (n = 196). These participants responded to the entire study, completing both the quantitative and qualitative components. Responses to open-ended questions were coded as binary, with 0 indicating "no" and 1 indicating "yes". Predictor variables included the Big Five personality traits, Dark Triad characteristics, and demographics such as age, education, gender, employment, and cybersecurity involvement. Each Random Forest model was optimized using 10-fold cross-validation, training on and testing on multiple data subsets to ensure generalization. The final models consisted of 500 decision trees, providing stable estimates of variable importance while minimizing overfitting to specific patterns in the dataset.

The model's performance was evaluated using overall classification accuracy, Area Under the Receiver Operating Characteristic Curve (AUC), and Pseudo R^2, to facilitate interpretation alongside the regression results. This evaluation included both logistic regression and nonlinear approaches, enabling comparison of their predictive strengths.

Across all behaviors, the Random Forest model exhibited moderate-to-strong discriminative ability, with AUC scores ranging from 0.73 to 0.85. These findings confirmed the overall reliability and applicability of the earlier regression results. The models predicting structured, creative, and sophisticated behaviors achieved the highest accuracy, ranging from 84% to 96%, consistent with previous logistic results. Among the predictor variables, Psychopathy and Machiavellianism were the most influential personality traits, followed by Conscientiousness and Extraversion.

Feature importance rankings, reflecting each predictor's relative contribution to the model's decision accuracy, revealed a clear hierarchy. Psychopathy had the highest average importance score (≈ 0.41), followed by Machiavellianism (≈ 0.28), Conscientiousness (≈ 0.24), and Extraversion (≈ 0.19). The Dark Triad traits were primarily driven by persistence, deception, and high-risk behaviors. The Big Five traits contributed to structured and creative behaviors. Demographic variables showed lower importance scores (≈ 0.10 – 0.15). This demonstrates that personality is the dominant predictive variable.

The Random Forest validation reinforced the core findings from the regression analyses, confirming that personality and other factors, such as age and experience, consistently predict intrusion behaviors. Psychopathy remained the most influential trait, particularly for persistence, boldness, and high-risk behaviors. Machiavellianism also showed high feature importance, indicating its ability to predict deception and calculated risk-taking behaviors.

The model identified Conscientiousness and Extraversion as strong predictors of both structured and creative behaviors. It suggests that organized, methodical attackers (highly Conscientious) and innovative, curious thinkers (highly Open and Extraverted) can be reliably identified through personality modeling.

The Random Forest validation strengthened the predictive validity of the regression models, thereby increasing confidence in the study's conclusions. By confirming that the strongest behavioral predictors remained stable across both approaches (regression models and Random Forest), the results indicate that personality typology has measurable, generalizable effects on intrusion decision-making.

The Random Forest validation strengthened the predictive validity of the regression models, thereby increasing confidence in the study's conclusions. By confirming that the strongest behavioral predictors remained stable across both approaches (regression and Random Forest), the results indicate that personality typology has measurable, generalizable effects on intrusion decision-making.

Quantitative and machine-learning analyses provided strong statistical evidence that personality traits influence cyber-intrusion behaviors. However, these models focus on structural patterns and overlook the subjective reasoning behind decisions. To gain a comprehensive understanding of how individuals perceive, justify, and adapt their decision-making in intrusion scenarios, a qualitative study was conducted. The open-ended responses from the tabletop exercise provided valuable context, shedding light on the cognitive processes, motivations, and situational judgments that underpin the quantitative findings.

Overall, the Random Forest validation shows that the main predictors identified in the regression analyses remained consistent across different analytic methods. This stable ranking of

predictor importance reinforces the robustness of the identified relationship between personality traits and intrusion behaviors and boosts confidence in the quantitative results.

Qualitative Findings

The qualitative aspect of the study aimed to deepen understanding by examining how participants thought about their decision-making and intentions during the simulated cyber intrusion. Although the statistical models identified measurable connections between personality traits and intrusion behaviors, the open-ended responses provided valuable insights into the actual actions taken.

A total of 196 participants completed the open-ended portion of the study, each providing a narrative describing the strategies they would use during different attack phases. The narratives were coded using a binary method to identify major categories aligned with MITRE ATT&CK and the hypotheses. The coding process followed an iterative approach based on Saldaña's (2015) thematic methods.

To ensure consistency and reliability in qualitative coding, a structured coding protocol was used. A detailed codebook was developed in advance based on the study's hypotheses, prior literature, and the MITRE ATT&CK Framework. The codebook includes operational definitions, inclusion criteria, and keyword indicators for each behavioral category, which are available in Appendix B.

A subset of responses was independently reviewed to assess coding consistency. Inter-rater reliability was measured using Cohen's kappa (κ), which quantifies agreement beyond chance. The high reliability score ($\kappa = 0.98$) indicated nearly perfect agreement, demonstrating strong consistency in applying coding rules. Any discrepancies were minor and resolved through discussion and clarification of the coding definitions before finalizing the coding. This process

ensured that qualitative responses were coded systematically and reproducibly across different behavioral categories.

As discussed, several coded behaviors were observed. Many responses contained multiple behaviors within a single reply, each marked with a unique code. For instance, one participant outlined a detailed, multi-stage reconnaissance strategy focused on stealth, OSINT, and targeting high-value access points. The response identified passive reconnaissance as the primary method, followed by infrastructure mapping, Social Engineering, preparation, and limited physical reconnaissance. Target prioritization centered on remote access, portal, and system account access, high-priority personnel, legacy systems, and third-party vendors. This response highlighted the exploitation of operational strain during crises while avoiding disruptive actions. The full participant's response is included in Appendix F.

The upcoming sections emphasize key qualitative themes identified in and examine them in detail. Direct quotations are incorporated to maintain the authenticity of participants' perspectives and illustrate how traits appear in decision-making. These qualitative insights aim to connect statistical patterns with psychological interpretations, providing a thorough understanding of how personality traits shape behavior and choices.

Thematic Frequencies and Overview

The qualitative data revealed clear behavioral patterns across the coded categories. Participants provided open-ended responses of varying lengths, allowing them to express multiple behavioral tendencies in a single response. Many described multi-phase intrusion strategies that integrated techniques such as reconnaissance, Social Engineering, and lateral movement within a single reply. The overall distribution of these behavioral themes is summarized in Table 20.

Table 20.

Distribution of Qualitative Behavioral Themes (N = 196)

Behavioral Theme	Percent of Responses	Description
Social Engineering	84.7%	Human-centric manipulation tactics, such as impersonation and deception
Structured	62.2%	Methodical, procedural, and organized attack approaches
Persistence	56.6%	Continued efforts to maintain or regain access despite obstacles
Creative	4.6%	Unconventional or adaptive tactics
Aggressive	3.8%	Disruptive or destructive tactics, such as ransomware

The most prevalent themes were Social Engineering (84.7%), followed by structured (62.2%) and persistence (56.6%). Creative and aggressive tactics were discussed less frequently, with both under 5%. Responses most commonly referenced impersonation, systematic reconnaissance, and iterative efforts to maintain access.

Table 21.

Behavioral themes, with example quote and associated personality traits

Behavioral Theme	Representative Quote	Associated Personality Traits
Social Engineering	"I would pose as IT support to gain credentials…"	Machiavellianism, Extraversion
Structured	"I would map the network before touching anything"	Conscientiousness
Persistence	"I'd keep trying different paths until it worked"	Psychopathy
Creative	"I'd use a headless device behind a TV"	Openness
Aggressive	"I'd deploy ransomware to disrupt operations"	Low Agreeableness, Psychopathy

As shown in Table 21, responses often mentioned impersonating staff, exploiting workflows within the targeted facility, and creating perceived trusted relationships to gain

access. One participant exemplified this, stating, “I would pretend to be a maintenance or delivery person and use that as an excuse to enter restricted areas.” Another participant said, “I would pose as IT support to request credentials or access from busy staff.” These responses demonstrate the common use of deception and persuasion to compromise a network. They align with traits like Machiavellianism and Extraversion.

Structured behaviors were also prominently highlighted. Participants often described systematic plans that showed organization, discipline, and compliance with established norms and best practices in common attack strategies. These behaviors align with Conscientiousness. Several participants mentioned performing reconnaissance methodically, for example, “I would start with network scanning, identify open ports, then escalate privilege once access is confirmed.” Others emphasized careful preparation, noting they would document every step and create checklists to ensure no phase was overlooked before moving on. This emphasis on procedures and methods indicates a desire for control and accuracy.

Persistence demonstrated a strong, resilient approach to overcoming technical and situational obstacles. One participant said they would create hidden backdoors for quick re-entry if discovered. Another explained that if detected, they would switch to passive techniques to blend with legitimate traffic until the observers lost track of their activity.

Creative and aggressive responses were less frequent, yet they provided valuable insights. One participant said, “I would attach a small headless device that blends into the network and exfiltrate data quietly.”

Aggressive tactics contrast with creative ones, involving intentional disruption or significant destruction. One participant said, “I would target HER systems with ransomware to cripple hospital operations.”

Overall, the qualitative distribution reflected the quantitative findings. This overview sets the stage for the following sections, which explore the behavioral categories in greater detail and demonstrate how personality-driven cognitive styles influence decision-making in cyber intrusion.

Thematic Patterns and Behavioral Dimensions

The qualitative responses provided rich insight into how personality relates to intrusion decision-making. Beyond frequency counts, the open-ended responses revealed how participants approached, rationalized, and adapted their actions during the simulated tabletop exercise. Many patterns emerged, reflecting cognitive tendencies, motivations, drivers, and strategic control that align with the quantitative findings.

The following sections outline the identified behavioral themes. Each theme is examined using participant quotes and linked to relevant personality predictors and quantitative results, providing a comprehensive view of how individual differences affect intrusion decision-making.

Structured and Reconnaissance

Structured and reconnaissance behaviors were frequently mentioned in the open-ended responses. These behaviors demonstrated organization, careful planning, and systematic approaches to targeting the environment. These qualities align with the regression model findings linking Conscientiousness to structured actions. The responses often emphasized logic, discipline, and the use of established techniques, such as those in MITRE ATT&CK, to carry out technical intrusions.

Qualitative responses described structured, reconnaissance-oriented behaviors, emphasizing deliberate, methodical planning before active intrusion attempts. Participants

consistently reported beginning with passive reconnaissance, including OSINT (Open-Source Intelligence) information gathering on organizational infrastructure, personnel, and exposed services, before progressing to more active scanning and probing. Responses highlighted careful attention to system configurations, user permissions, and access pathways. This reflected a preference for low-noise, controlled approaches that minimize detection risk. Appendix F presents participant responses illustrating these structured, reconnaissance-oriented strategies.

Manipulative and Deceptive

The next set of observed behaviors was deceptive, persuasive, and psychologically manipulative. These tactics resemble Social Engineering used in real-life cyber intrusions (Table 22). Participants often described leveraging credibility, trust, and psychological manipulation to gain unauthorized access rather than relying solely on technical exploits. They explained that they impersonated legitimate users, contractors, or other seemingly "normal" actors in the environment, such as delivery personnel or patients. This allowed them to exploit trust and craft convincing narratives to bypass both technical and physical security barriers.

Table 22.

Social Engineering Quotes

"This looks easy. Just send someone wearing scrubs, someone holding a pizza, or someone wearing overalls and a toolbox. It's easy enough to get into facilities when they're functioning well, let alone when everyone is distracted and exhausted. Just have them go on their way to the required location and, if someone asks, say you're going to check patient files, deliver pizza, or fix the server room. If someone gets suspicious, have them call the nr you bring saying that the boss is doing a pentest with people on the other side pretending theyre the boss to confirm the pentest and allow them entrance wherever they want."
"I would imitate a call (social engineer) as a high level security official and assure them the threat was an error and to ignore."
"I would try to phish them via email by pretending to be a doctor dire need of files for a sick patient, and provide a link that would exploit their machine."
"To stay inside the hospital's system without getting caught, I'd first trick a staff member into giving me their login through a fake but convincing email."
"Use emotional and/or financial appeals to gain trust of my targets."

Participants often emphasized that influencing people is easier than compromising technology systems. The open-ended responses showed awareness of human vulnerability. They frequently discussed how emotion, authority, and current circumstances, such as targeting exhausted and overworked staff, may be the easiest way to gain unauthorized access.

Interestingly, the manipulative tactics were not always described as purely malicious or antisocial. Many participants viewed manipulative tactics as a strategic skill that requires emotional intelligence, confidence, and adaptability. For example, one participant wrote, "You just have to get them to trust you. Even the CEO and IT staff are just as vulnerable. Pretend to be someone they can trust. Send them a link. They click it. And there you go." This quote demonstrates the opportunism common among Machiavellian individuals. Many Social Engineering tactics are paired with social assertiveness, which is associated with Extraversion—this blend of strategic intent and interpersonal engagement.

The participants' responses highlight cognitive flexibility, a hallmark of Openness and Extraversion. Participants frequently discussed the need to adapt personas and stories on the fly, especially as the pressure of potential detection increased. This was often reflected in changes in tactics, particularly when using in-person physical reconnaissance. For example, one participant said they would act lost inside the building if they sensed suspicion from others.

Some participants described their behavior as a form of psychological role-playing, in which they rely on reading cues from the people they are targeting and adjust as they learn more. This pattern of development shows that this is not merely an extension of the Dark Triad manipulation traits but a manifestation of situational intelligence, in which one can adapt to various circumstances as they arise.

Interestingly, even those with low levels of Machiavellianism described adopting deceptive roles out of necessity. Deception was often used strategically. One participant low in Machiavellianism explained that it is not about lying; it is about playing a role to get the job done. This shows that manipulation is not necessarily a trait; though it can, it can also depend on the situation. This reinforces that while traits influence behavior, so do context, circumstances, and purpose.

Manipulative and deceptive behaviors demonstrate how psychological tactics enhance technical strategies. The high prevalence of Social Engineering in the dataset reflects real-world adversary campaigns in which attackers target humans before exploiting technology. These behaviors link the Dark Triads' focus on strategic self-interest with the Big Five's emphasis on interpersonal skills, suggesting that effective intrusions require balancing emotional intelligence and moral disengagement. These insights suggest that threat modeling requires a dual focus on

technical and human factors. Defenders must not only predict an attacker's technical moves but also understand how they think, persuade others, and adapt across environments.

Aggressive and High-Risk

A smaller but notable subset of participants exhibited aggressive or high-risk intrusion behaviors. These participants described actions intended to disrupt and assert dominance, with little concern for potential detection. The tactics they employed often posed significant danger to themselves, such as impersonating a high-ranking official. Unlike strategic manipulation, these tactics often reflected impulsivity, confrontation, and defiance, behaviors associated with psychopathy and Neuroticism.

Intense, damage-oriented actions characterize aggressive behavior. These behaviors aim to inflict serious harm, such as shutting down systems, deleting data, or causing ongoing disruption. Multivariate analyses revealed that aggression has a moderate ability to predict certain outcomes, correlating with higher Neuroticism and lower Agreeableness. This appears to be a key psychological indicator. The results suggest that aggressive actions stem from a combination of emotional reactivity and hostility (Neuroticism) and prosocial behaviors and empathy (low Agreeableness). Together, these traits create a profile of an attacker who may favor retaliatory and destructive tactics rather than stealthy or exploratory approaches.

Qualitative responses supported this pattern. For instance, one participant stated, “I would move to mass destruction.” Another participant noted that shutting down power disrupts everything. However, another wrote, “I would go straight for the core systems. No point hiding if the goal is impact.” Some participants specifically described running brute-force scripts and persisting until they reach their target. Another said, “We run and gun!” These statements reflect

an attitude of bold persistence and emotionally charged tactics. This aligns with high impulsivity and low empathy.

Others saw these tactics as a tool to achieve a goal. They described them as methods to distract or cause chaos within the organization, making it harder for defenders to intervene. For instance, one participant mentioned, “Create a disruption or distraction elsewhere…this is to increase their workload and spread their attention.” This shows that aggressive tactics, although occasionally impulsive, can also be used intentionally and strategically.

Even though aggressive tactics were used less often, they still had serious consequences. Participants reported using malware, ransomware, wiping data, and causing significant operational disruptions to the target environment.

High-risk behaviors are actions that increase the likelihood of detection or compromise personal security. Examples include loud network scanning, targeting high-profile individuals, and physical breaches. Multivariate regression analysis indicated moderate predictive ability, with Machiavellianism emerging as a significant positive predictor. Conversely, age was negatively correlated, indicating that younger participants were more likely to select high-risk strategies than older participants.

Qualitatively, many quotes reflected high-risk behavior. Those employing high-risk tactics often overlooked the chance of being caught and frequently claimed it would be “easy.” For example, one participant said, “It would be easy to penetrate as a patient. They would be too busy to notice me.” Another mentioned, “I would get lost looking for a bathroom, but it would actually be me searching for access points.”

High-risk behaviors present a paradox for defenders: they are harder to detect and more surprising. For instance, one participant said they would wear a disguise and pose as a

maintenance worker, claiming to be hired for repairs if questioned. In this role, they would seek out server rooms or exposed machines to target.

Creative and Sophisticated

Creative and sophisticated responses emphasized novel problem-solving strategies, experimentation, and adaptability in the face of dynamic obstacles. They represented inventive rather than purely procedural approaches.

Those who demonstrated creative thinking often employed unconventional or cross-domain approaches that deviated from standard procedures. These individuals frequently described using features unique to the hospital setting in the scenario, such as being a patient, leveraging TV or phone systems as the initial entry point, and focusing on third-party vendors, such as laboratories or pharmacies. Others mentioned quickly pivoting to compromising the pharmacy or medical labs. The participants often showed Openness to new experiences and cognitive flexibility.

In contrast, sophisticated behaviors required precision and multi-step plans (Table 23). These responses were highly technical, often described layered approaches.

Table 23.

Example Sophisticated Response

Primary Method to Maintain Access While Avoiding Detection:

Use a Low-and-Slow, Phishing-Based Initial Access Vector Paired with Stealthy Persistence Techniques

1. Initial Access – Phishing with Weaponized Document or Link
   - Craft a highly convincing spear-phishing email tailored to the hospital environment (e.g., COVID policy update, schedule change, vaccine alert).
   - Embed a malicious macro or link to an external payload hosted on a compromised site or trusted service (e.g., Dropbox, SharePoint clone).
   - Take advantage of email overload and user fatigue—staff are more likely to click or enable macros without scrutiny.

2. Establish Persistence – Covert and Non-Invasive

Once access is gained, choose one or more stealthy persistence methods, such as:
   - WMI Event Subscriptions – Difficult to detect and doesn't leave obvious startup entries.
   - Registry Run Keys or Scheduled Tasks with random names/timings to mimic normal OS behavior.
   - Living Off the Land Binaries (LOLBins): Use built-in Windows tools like certutil, powershell, or rundll32 to maintain access without dropping suspicious binaries.

3. Command & Control (C2) – Low Noise
   - Use encrypted, intermittent beaconing (e.g., over HTTPS or DNS tunneling) to communicate with your C2 server.
   - Set long sleep intervals and jitter to reduce traffic patterns and avoid detection by anomaly-based detection tools.

Persistence

Persistence was a key behavioral pattern in the qualitative data, reflecting a mindset of continuous effort and an unwillingness to give up on the goal despite obstacles, detection, or setbacks. It emphasized determination and the capacity to remain within the network even after initial tactics failed. The quantitative data indicated that Psychopathy significantly predicted persistence (OR = 1.40, $p = 0.041$), offering strong empirical support for this theme. Individuals with higher psychopathy scores tend to exhibit fearlessness, a desire for dominance, and low

sensitivity to potential punishment (Paulhus & Williams, 2002). These traits allow them to keep pursuing their goals despite risks, detection, or deterrence.

The link between Psychopathy and persistence suggests that, in the context of intrusions, it is not merely technical but also a psychological expression of resilience and control. Those who exhibit this behavior often view their actions as a challenge rather than a violation of boundaries. For example, one participant wrote, “I would just search all assets in the network for vulnerabilities. I would keep looking until I found one.” The statement reflects a cognitive preference for mastery and problem-solving, which relates to confidence and goal fixation.

Some participants with high Psychopathy scores offered notable responses, describing methods to maintain access and evade detection, often with confidence that simple adjustments would allow them to continue their activities. For example, one respondent stated, “Once detected, to continue operating undetected, I would shift tactics. Maybe ransomware. Maybe stealing data quietly for longer-term exploitation.” Another participant said, “I would just make a firewall so nobody can see me.” However, another mentioned, “If I think they are on to me, I would just lie low. Then resume operations in off-hours when they are not watching.” These comments reflect pragmatic persistence, treating obstacles as puzzles rather than deterrents or boundaries.

Interestingly, persistence also appears linked to strategic patience. Some participants emphasized the importance of staying stealthy until the right moment. For example, one participant stated, “When detection is suspected, I will stop all active operations and rely on stealthy persistence methods like WMI or scheduled tasks on low-visibility systems.” Another said, “Change users and lay low. Look to launch attacks that are difficult to trace.” This shows that persistence is not always overt; it can involve waiting for the right opportunity. The nuanced

findings about persistence suggest it exists on a spectrum, highlighting the nature of psychopathy, which can be both bold and strategic.

Summary

The results of this mixed-methods study indicate that a combination of personality traits and contextual factors influences decision-making about cyber intrusions. Quantitative analyses showed that traits from both the Dark Triad and Big Five frameworks significantly predicted patterns of intrusion behavior, although no single trait was deterministic. Psychopathy and Machiavellianism emerged as the strongest Dark Triad predictors, particularly in relation to persistence, deception, and high-risk tactics. Among the Big Five traits, Conscientiousness and Openness were most consistently associated with structured and creative intrusion approaches, respectively.

Demographic variables further shaped these relationships, with age and cybersecurity involvement influencing behavioral tendencies and model performance. Younger participants were more likely to engage in bold, high-risk behaviors, whereas greater technical experience was associated with more organized and sophisticated intrusion strategies.

Qualitative findings complemented the quantitative results by showing that intrusion behaviors were dynamic and multi-layered rather than isolated or sequential. Participants frequently described adaptive strategies that combined multiple tactics, reflecting the hybrid nature of real-world cyber intrusions. Together, the quantitative and qualitative analyses show that intrusion behaviors emerge from the interaction of dispositional traits, experience, and situational context.

DISCUSSION

This chapter examines the study's results in relation to the research hypotheses, relevant theories, and existing literature on personality and cybersecurity behavior. It aims to interpret how the Dark Triad and Big Five traits influence decision-making during cyber intrusions in a simulated attack setting. Using a mixed-methods approach, the discussion integrates quantitative models with qualitative insights to explore how personal differences shape intrusion-related behaviors.

Overview of Findings

This study suggests that personality traits significantly influence decisions about cyber intrusion, though their impact varies by behavioral type and context. Generally, Dark Triad traits showed stronger and more consistent links to intrusive and risky behaviors. In contrast, Big Five traits were more associated with organized, methodical, and creative strategies.

Psychopathy emerged as the strongest predictor of persistent, bold, deceptive, and high-risk intrusion behaviors. Machiavellianism consistently correlated with calculated, goal-driven intrusion tactics. Conversely, Big Five traits such as Conscientiousness and Openness were associated with organized reconnaissance, systematic execution, and creative or adaptable strategies. These patterns reflect differences in cognitive styles rather than malicious intent. These findings were consistent across correlational analyses, regression models, and machine learning validation, strongly supporting the study's conclusions.

Qualitative responses supported the statistical findings by revealing how participants understood and justified their intrusion strategies. They often described multi-step approaches, adaptive decision-making, and persistent effort toward their goals. These narratives provided

insight into the reasoning behind the quantitative data, highlighting how personality traits influenced planning, risk-taking, manipulation, and strategic changes during intrusion scenarios.

In addition to personality traits, demographic and experiential factors also influenced intrusion behaviors. Age and cybersecurity involvement moderated links between personality and behavior, indicating that intrusion decision-making results from an interaction between stable traits and context. These findings highlight the need to analyze cyber intrusion behaviors through a person-situation interaction model rather than viewing behavior solely as a result of personality traits.

Although observed relationships were statistically significant, the overall effect sizes remained small. This pattern is consistent with behavioral research on complex human decision-making, in which outcomes typically result from the interaction among multiple psychological, situational, and contextual factors rather than from a single dominant element (Mischel & Shoda, 1995). Cyber intrusion behavior is shaped not only by personality traits but also by technical expertise, environmental constraints, and experimental knowledge. Therefore, personality should be viewed as a probabilistic factor that influences behavioral tendencies rather than a deterministic predictor of intrusion behaviors.

Hypothesis 1: Dark Triad Traits and Intrusion Behaviors

The Dark Triad traits (Machiavellianism, Narcissism, and Psychopathy) emerged as key predictors of cyber intrusion behaviors in both quantitative and qualitative analyses, supporting Hypothesis 1. While recent literature has expanded this model to include the Dark Tetrad by adding everyday sadism as a distinct but related dimension of socially aversive personality, this study was designed, and data collection started when the Dark Triad was still the primary and most widely used model (Paulhus, 2014). As a result, sadism was not measured in this study.

Current research indicates that sadistic tendencies could offer additional insight into malicious or harm-driven behaviors in cyber settings (Buckels et al., 2013; Furnham et al., 2024; Gómez-Leal et al., 2024); however, the findings should be understood within the framework of the Dark Triad, which was well established at the time of the study's design.

Overall, the Dark Triad personality traits accounted for meaningful variation in intrusion behaviors, particularly deception, persistence, and risk tolerance. Importantly, these findings do not suggest that participants exhibit clinical levels of psychopathy or maladaptive personality pathology. Rather, they indicate that higher relative levels of socially aversive traits within a normative range were associated with a greater likelihood of selecting bold, manipulative, and risk-oriented intrusion strategies.

While the Big Five traits primarily reflected differences in cognitive style and behavioral organization, the Dark Triad traits captured motivational tendencies related to dominance, emotional detachment, and strategic exploitation. In line with Hypothesis 1, individuals scoring higher on Dark Triad dimensions were more inclined toward intrusive behaviors characterized by persistence, deception, and elevated risk, suggesting that even subclinical expression of these traits can shape cyber decision-making patterns.

Among the Dark Triad traits, Psychopathy showed the most consistent and robust association with intrusion behavior across models. In binary logistic regression analyses, Psychopathy significantly predicted persistent intrusion behavior (OR = 1.40, $p = 0.041$), indicating that higher Psychopathy scores were linked to a greater likelihood of continuing an intrusion despite deterrence or detection. Across multivariate models, Psychopathy also showed a consistently positive association with bold, high-risk, and sophisticated behaviors, supporting its broader role in tenacity, dominance-seeking, and resilience under pressure. Qualitative

responses reinforced this pattern, with participants describing repeated attempts, adaptive strategy shifts, and a willingness to persist until a viable access point was identified. The narratives suggested that Psychopathy-related behaviors are goal-directed and relatively unimpeded by fear or anxiety.

Importantly, although Psychopathy did not emerge as a statistically significant predictor of sophisticated intrusion behaviors in the multivariate logistic regression model, the direction and pattern of its associations remain conceptually consistent with Hypothesis 1. Psychopathy was a significant predictor of persistence, boldness, and high-risk strategies across multiple behavioral models, indicating a broad influence on intrusion engagement rather than on technical complexity alone.

This suggests that Psychopathic traits may shape how individuals sustain effort, tolerate risk, and remain emotionally detached during intrusion attempts, rather than directly determining the sophistication of specific tactics. In practice, these dispositional characteristics may indirectly facilitate complex operations by supporting endurance, adaptability, and sustained engagement over time, particularly when combined with technical skill or a tendency toward structured planning.

Accordingly, while Psychopathy does not independently predict sophisticated behavior, it appears to function as a contributing psychological factor that amplifies sustained, high-intensity intrusion activity, consistent with the motivational mechanisms proposed in Hypothesis 1.

Moderation analyses further clarified the contextual nature of this relationship. The influence of Psychopathy on persistence was strongest among younger participants and declined with age. This pattern suggests that developmental factors, such as increased self-regulation and experience, may attenuate impulsive tendencies over time. It aligns with longitudinal research

demonstrating age-related declines in impulsivity and sensation-seeking (Stoltenberg et al., 2008). In a cyber intrusion context, increased age and experience may temper the risk-taking aspects of Psychopathy while preserving its association with persistence and emotional detachment.

Machiavellianism also emerged as an important predictor of intrusion behavior, particularly deception and calculated risk-taking. In multivariate models, Machiavellianism positively predicted the use of deceptive strategies. Age showed an inverse relationship with high-risk behaviors, indicating that younger individuals with higher Machiavellianism were more likely to employ risky, strategically motivated tactics. These findings align with the conceptualization of Machiavellianism, characterized by strategic manipulation, long-term planning, and goal-oriented deception (Jones & Paulhus, 2014).

Qualitative findings further reinforced the interpretation of Machiavellianism. Participants frequently described impersonation, trust exploitation, and Social Engineering tactics to manipulate human vulnerabilities. Statements such as “Pretend to be someone they can trust. Send them a link. They click it. And there you go” reflect the calculated opportunism associated with Machiavellian tendencies. Unlike Psychopathy, which manifested as impulsive persistence, Machiavellianism appeared to operate through deliberate, cognitively controlled deception. Age-based moderation analyses suggested that Machiavellianism may shift from impulsive manipulation in younger individuals to increasingly refined and strategic deception later in adulthood, reflecting a transition from “hot” to “cold” manipulation (Jones & Paulhus, 2017).

Narcissism showed comparatively weaker predictive power across models but remained relevant in specific behavioral contexts. In the ransomware context, Narcissism was positively

associated with confidence-driven exploitation (Pseudo $R^2 = 0.15$; Accuracy = 84%). Narcissistic traits, including self-importance, a desire for admiration, and sensitivity to threats (Paulhus & Williams, 2002), may motivate status-seeking behaviors that emphasize visibility, dominance, and perceived impact. Participants exhibiting this pattern often described targeting systems or assets of high symbolic or operational value. This suggests that ego-driven motives may underlie certain forms of exploitative cyber behavior.

Taken together, the Dark Triad findings support a multidimensional model of intrusion decision-making. Psychopathy contributes to boldness and persistence through emotional detachment and reduced threat sensitivity. Machiavellianism enables calculated deception and strategic risk-taking through deliberate manipulation. Narcissism amplifies motivational intensity and the pursuit of recognition and dominance. These traits did not operate in isolation. Correlational analyses revealed substantial interrelationships among the three dimensions, suggesting that intrusion behaviors often reflect a synergistic combination of confidence, adaptability, and a willingness to exploit both technical systems and human vulnerabilities.

Hypothesis 2: Openness, Creativity, and Sophistication

Hypothesis 2 proposed that those higher in Openness would be more likely to engage in creative and exploratory intrusion behaviors. This hypothesis was supported. Openness was strongly positively associated with creative intrusion tactics and inversely related to rigid, structured approaches, indicating that highly open individuals favor flexibility, experimentation, and unconventional problem-solving strategies during cyber intrusions.

Analyses showed that Openness was negatively correlated with structured behavior ($r = -0.18$; $p = 0.014$) and positively associated with creative intrusion outcomes. The creative model demonstrated strong explanatory power (Pseudo $R^2 = 0.28$; Accuracy = 96%). These findings

align with broader psychological research linking Openness to divergent thinking, intellectual curiosity, and tolerance for ambiguity (McCrae & Costa, 1997). In the context of cyber intrusions, these traits appear as a willingness to experiment with novel attack vectors, explore alternative pathways, and adapt to rapidly changing constraints.

Qualitative responses strongly reinforced this interpretation. Participants high in Openness frequently described uncovering overlooked vulnerabilities, experimenting with unconventional tactics, or treating the intrusion as a dynamic problem-solving exercise rather than a fixed technical sequence. These narratives suggest that highly open individuals conceptualize intrusions as exploratory challenges, prioritizing creativity and adaptability over procedural adherence. Such cognitive styles closely resemble those observed in ethical hacking and penetration testing contexts, where innovation and curiosity are critical for identifying previously unknown weaknesses and vulnerabilities.

Although Openness is linked to exploratory and creative actions, its role in advanced intrusion techniques seems indirect. Instead of directly increasing technical complexity via structured planning, Openness fosters flexibility and adaptive thinking, which can enhance sophistication when paired with technical skills or organizational abilities. In this way, Openness influences how attackers explore options rather than how they perform complex operations.

Extraversion also emerged as a complementary predictor in creative intrusion models. While Openness accounted for the cognitive dimension of creativity, Extraversion appeared to shape how creative tendencies were expressed behaviorally. Individuals higher in Extraversion may be more willing to take initiative, actively test new tools, and persist through trial-and-error exploration.

Openness and Extraversion together define a behavioral profile marked by curiosity-driven thinking and active participation. This blend fosters creative intrusion decision-making by facilitating both idea generation and implementation. These results support Hypothesis 2, indicating that creative intrusion behaviors are rooted in personality-driven exploratory tendencies rather than solely technical or procedural motives.

Hypothesis 3: Conscientiousness and Structured Approaches

Hypothesis 3 proposed that individuals higher in Conscientiousness would favor structured, methodical, and low-risk intrusion approaches. Overall, the findings provided partial support for this hypothesis. Conscientiousness showed consistent directional relationships with structured and reconnaissance behaviors across quantitative and qualitative analyses, indicating reliable behavioral patterns, even when some effects did not reach conventional thresholds for statistical significance.

Quantitative results showed that Conscientiousness was positively associated with reconnaissance and structured intrusion behaviors. Although the effect for reconnaissance narrowly missed traditional significance (OR = 1.49, $p = 0.06$), the direction and magnitude of the relationship were consistent with expectations. In the multivariate models, Conscientiousness contributed meaningfully to predictive accuracy for both structured behaviors (Pseudo $R^2 = 0.30$; Accuracy = 92%) and sophisticated behaviors (Pseudo $R^2 = 0.17$; Accuracy = 91%). This suggests that highly Conscientious individuals possess the cognitive organization required for systematic, multi-phased intrusion strategies.

Qualitative findings strongly reinforced this pattern. Participants whose responses reflected structured decision-making frequently described careful planning, documentation, verification, step-by-step verification, and execution. These individuals emphasized passive

reconnaissance, low-noise scanning, and deliberate progression rather than rapid or opportunistic actions. Such narratives reflect a procedural mindset characterized by attention to detail, preparation, and control.

These findings align with established personality theory, which characterizes Conscientiousness as involving self-discipline, organization, persistence, and goal-oriented behavior (Costa & McCrae, 1992). In cybersecurity contexts, these traits closely align with behaviors observed in professional penetration testing and defensive security roles, where adherence to structured methodologies and frameworks, such as MITRE ATT&CK, is common. The present findings suggest that these same dispositional qualities can support structured intrusion behaviors in adversarial scenarios when ethical constraints are removed.

The results indicate that Conscientiousness does not merely promote cautious or rule-abiding behavior. Rather, it supports disciplined execution, regardless of moral framing. Highly Conscientious individuals appear motivated by order, precision, and task completion, which can facilitate effective intrusion behaviors when aligned with offensive goals. This supports Hypothesis 3 by showing that Conscientiousness shapes how intrusions are carried out, favoring controlled, systematic approaches over impulsive, high-risk tactics.

Hypothesis 4: Extraversion and Social Engineering

Hypothesis 4 proposed that higher levels of Extraversion would be associated with a greater preference for Social Engineering and interpersonal intrusion tactics. The findings provided partial support for this hypothesis. Although Extraversion did not emerge as a statistically significant predictor across all quantitative models, it showed a consistent positive relationship with bold and socially engaged intrusion behaviors.

In the logistic regression analyses, Extraversion was positively associated with bold intrusion tactics (OR = 1.63), indicating that individuals higher in Extraversion were more likely to use assertive, direct, and action-oriented strategies. This pattern aligns with established personality theory, which characterizes Extraversion as involving sociability, assertiveness, stimulation-seeking, and confidence in interpersonal engagement (John & Srivastava, 1999). In the context of cyber intrusions, these traits may predispose individuals toward tactics that involve interaction, persuasion, and initiative rather than passive or covert approaches.

Qualitative findings strongly reinforced this interpretation. Social Engineering emerged as the most prevalent behavioral theme across participant responses, underscoring the central role of human-centered manipulation in intrusion decision-making. Participants frequently described impersonating trusted individuals, exploiting organizational workflows, and initiating direct contact with targets to gain access. These narratives reflect behaviors that rely on confidence, verbal assertiveness, and comfort with interpersonal deception.

Although Extraversion's effects were modest in magnitude and did not reach statistical significance across all models, the convergence of quantitative trends and qualitative evidence suggests that Extraversion shapes how intrusion behaviors are enacted rather than whether they occur. Extraverted individuals may be more inclined to initiate contact, escalate interactions quickly, and exploit social dynamics, making them particularly well-suited to Social Engineering tactics. These findings provide partial support for Hypothesis 4 and underscore the importance of considering interpersonal personality traits when examining intrusion strategies that rely on human manipulation rather than purely technical exploitation.

Hypothesis 5: Aggression, Risk, and Low Agreeableness

Hypothesis 5 proposed that lower Agreeableness would be associated with more aggressive, independent, and risk-oriented intrusion behaviors. The findings provided partial support for this hypothesis. Across multiple models, Agreeableness showed a consistent inverse relationship with intrusion behaviors that reflect autonomy, persistence, and reduced concern for social or ethical constraints.

In the multivariate logistic regression analyses, Agreeableness showed consistent protective effects across intrusion behaviors. Agreeableness was a significant negative predictor of structured intrusion behavior ($\beta = -2.01$, $p = 0.001$), indicating substantially lower odds of engaging in systematic and forceful attack strategies among more agreeable individuals. It also significantly predicted a lower likelihood of lateral movement across network environments ($\beta = -0.79$, $p = 0.023$). These findings suggest that individuals higher in agreeableness are less inclined toward intrusive, persistent, and self-directed exploitation tactics, consistent with their cooperative and conflict-avoidant dispositions.

This pattern aligns with prior personality research, which characterizes low Agreeableness as marked by competitiveness, skepticism, emotional detachment, and reduced concern for interpersonal consequences (Paulhus & Williams, 2002). In the context of cyber intrusion decision-making, these traits may facilitate tactical independence, resistance to social inhibition, and a willingness to operate in ambiguous or adversarial environments. Such qualities can support behaviors that prioritize task completion and control over relational or reputational considerations.

Neuroticism demonstrated a more complex, secondary pattern. Rather than directly predicting aggression or risk-taking, Neuroticism appeared to interact with persistence-related behaviors under pressure. Models linking Neuroticism to persistence and emotional activation

(Pseudo $R^2 = 0.21$; Accuracy = 73%) suggest that heightened emotional reactivity may intensify behavioral engagement when individuals encounter resistance or perceived threat. While Neuroticism is traditionally associated with anxiety and avoidance (McCrae & Costa, 1997), in high-takes intrusion scenarios, emotional arousal may instead manifest as increased fixation or difficulty disengaging from the task.

Importantly, Neuroticism did not emerge as a primary driver of aggressive intrusion strategies. Instead, its influence appeared conditional and situational, potentially amplifying stress responses rather than shaping strategic intent. In contrast, low Agreeableness more directly aligned with the core mechanisms proposed in Hypothesis 5, supporting its role in facilitating adversarial, self-reliant, and norm-resistant intrusion behaviors.

Demographic Moderators and Contextual Effects

Demographic variables, such as age and cybersecurity involvement, were explicitly tested as moderators of the link between personality traits and intrusion decision-making by including interaction terms in the regression models. These tests assessed whether the strength or direction of personality-behavior relationships varied across demographic groups, rather than determining whether demographics directly explained these relationships. The results showed that personality traits provided a consistent dispositional basis for intrusion behavior. At the same time, factors such as age and professional involvement influenced the extent to which these traits manifested during a simulated cyber intrusion exercise.

Importantly, these demographic variables were not treated as mediators in this study because the research design and analyses were not set up to test indirect causal pathways. Instead, age and cybersecurity involvement served as contextual moderators, influencing how personality-driven behaviors are expressed by amplifying or limiting tendencies in risk-taking,

persistence, and strategic decision-making. This approach aligns with a person-situation interaction framework, in which stable personality traits interact with developmental and experiential factors to shape behavior.

Age was an important factor shaping links between personality traits and behaviors. Analyses showed that the association between Psychopathy and ongoing intrusive behaviors varied by age. Notably, stronger links between Psychopathy and persistence were observed in younger individuals, while the association weakened with age. Younger people were more prone to risk-taking, bold actions, and persistent behaviors despite deterrents, whereas older adults displayed greater restraint and behavioral control.

This pattern aligns with developmental research indicating that impulsivity and sensation-seeking decline across adulthood as self-regulation develops (Stoltenberg et al., 2008). In the context of cyber intrusion decision-making, age appears to shape how psychopathic tendencies are expressed, attenuating persistent and high-risk behaviors over time rather than eliminating underlying dispositional traits.

Cybersecurity involvement also served as a key contextual moderator across several models. Defined as professional or academic engagement in the cybersecurity field, this variable significantly improved predictive accuracy for both structured behaviors (Pseudo $R^2 = 0.30$; Accuracy = 92%) and sophisticated behaviors (Pseudo $R^2 = 0.17$; Accuracy = 91%). These findings indicate that technical training and domain-specific expertise interact with personality traits to influence intrusion decision-making, particularly for behaviors that require planning, coordination, and technical precision.

Participants with greater cybersecurity involvement frequently demonstrated methodical planning, use of specialized tools, and advanced understanding of network architecture in their

qualitative responses. These patterns suggest that professional exposure shapes how personality traits are expressed rather than serving as an independent driver of behavior. For example, individuals high in Conscientiousness or Openness were more likely to translate these traits into technically complex or innovative intrusion strategies when supported by relevant expertise.

Taken together, these findings support a person-situation interaction framework for understanding cyber intrusion behaviors. Personality traits provide relatively stable predispositions, whereas demographic factors, such as age and professional involvement, shape the situational conditions under which those traits are expressed. Rather than mediating, these demographic variables function as moderators that amplify, constrain, or redirect personality-driven behaviors depending on the developmental context and expertise.

From an applied perspective, these results highlight the potential value of workforce development, ethical training, and mentorship in shaping how personality traits manifest in cybersecurity contexts. By providing structure, accountability, and professional norms, organizational environments may help channel risk-oriented or dark personality traits toward constructive, security-focused practices rather than adversarial misuse.

Integration of Quantitative and Qualitative Findings

Integrating quantitative and qualitative findings provides a clearer picture of how personality traits influence decision-making in cyber intrusions. Statistical models revealed significant, directional links between traits and specific intrusion behaviors, while qualitative data showed how these traits manifest in real-world contexts. Together, the results indicate that personality shapes both the selection of behaviors and their execution and adaptation over time.

Quantitative analyses often modeled intrusion behaviors as discrete outcomes; however, qualitative responses consistently showed that participants viewed intrusions as dynamic, multi-

phase processes. Individuals often described shifting among reconnaissance, deception, persistence, and adaptation within a single response. This helps explain why multiple traits contributed to overlapping behavioral categories in the statistical models and why effect sizes were modest yet consistent across behaviors. Personality traits appeared to influence behavioral style rather than isolated tactical choices.

The qualitative data also contextualized indirect quantitative findings. For example, traits such as Psychopathy and Extraversion did not consistently emerge as statistically significant predictors across models. Yet participant narratives showed that emotional detachment, confidence, and assertiveness supported persistence, boldness, and the use of Social Engineering strategies. These accounts clarify how personality traits may exert influence through indirect or situational pathways that linear statistical models do not fully capture.

Overall, the convergence of quantitative and qualitative evidence supports a person-situation interaction model for cybersecurity intrusion behavior. Personality traits offer stable dispositional tendencies, while situational factors and task demands influence their expression. Combining both methods confirms that intrusion decision-making is not driven solely by technical skills but rather involves a complex interplay among cognitive styles, emotional regulation, motivation, and contextual factors.

Importantly, these findings should not be interpreted as suggesting that personality traits alone enable individuals to carry out intrusions. Technical expertise, access to tools, and domain knowledge remain essential prerequisites for conducting intrusion activities. Instead, personality traits seem to influence how technically capable individuals approach decision-making within an intrusion context. Traits shape procedural style, escalation sensitivity, persistence, and risk

tolerance, while technical expertise determines the feasibility and execution of intrusion behaviors.

The integration of quantitative and qualitative results can be understood through well-established behavioral frameworks that focus on motivation, intention, and contextual influences. For instance, UTAUT/UTAUT2 show how behavioral intention is affected by perceived usefulness, effort, social influence, and facilitating conditions (Venkatesh et al., 2012). Patterns observed in this study, including those linked to creative, structured, and Social Engineering behaviors, mirror these decision-making processes. Traits such as Openness and Extraversion seem to correspond with cognitive flexibility and social confidence, supporting exploratory and socially driven intrusion methods. In contrast, Dark Triad traits represent motivational factors related to dominance, stimulation, and reward-seeking.

Similarly, the Theory of Planned Behavior offers a useful framework for understanding why participants engaged in intrusion behaviors despite recognizing potential risks (Maasberg et al., 2015). In qualitative responses, participants often expressed a strong intention to act, frequently justifying their choices based on perceived opportunity, necessity, or control. Traits such as Machiavellianism and Psychopathy appear to strengthen behavioral intention by reducing normative constraints and increasing perceived control, which helps explain the persistence and risk-taking observed in the quantitative data.

The findings also support the Capability Means Opportunity (CMO) framework, highlighting that behaviors result from the interplay of personal capability, available means, and situational opportunity (Gaia et al., 2020). In this research, cybersecurity engagement fostered the development of complex behaviors, underscoring the importance of technical skills.

Meanwhile, dark personality traits such as Machiavellianism and psychopathy often served as motivational factors that enabled individuals to take advantage of opportunities.

Finally, the Routine Activity Theory (RAT) explains behavior within everyday opportunity structures (Rege, 2013). Participants highlighted the exploitation of predictable workflows, unmonitored systems, and trust-based human vulnerabilities, showing how personality influences motivation and operates within routine organizational settings. Collectively, these frameworks offer complementary perspectives on the findings, demonstrating how personality traits, motivations, and situational factors interact to influence decisions about cyber intrusions.

Psychological Profiles of Cyber Intrusion Behavior

The results suggest that cyber intrusion behaviors may reflect distinct cyber-personality profiles rather than behaviors operating in isolation. Although the study does not establish a formal classification, consistent patterns in both quantitative and qualitative data indicate that certain combinations of personality traits, motivations, and contextual factors tend to co-occur systematically during intrusion decision-making.

For example, people with high levels of Psychopathy and Machiavellianism, particularly when combined with low Agreeableness, consistently demonstrate persistence, deception, and a willingness to take risks. This pattern reflects a dominant, goal-driven intrusion style characterized by emotional detachment and strategic manipulation. In contrast, individuals high in Conscientiousness involved in cybersecurity tend to use more organized methods, focusing on planning, detailed research, documentation, and procedural control. These behaviors showcase a technically disciplined approach that values accuracy over opportunism.

Individuals high in Openness, especially when paired with Extraversion, showed creative, exploratory, and adaptable intrusion styles that often involved experimentation, improvisation, and unconventional problem-solving. This indicates a cognitively flexible approach that values innovation rather than strict adherence to established methods. Importantly, these profiles were not mutually exclusive, as many participants exhibited a mix of traits that varied with the situation, perceived constraints, experience, and the tasks at hand.

The patterns largely align with a person-situation interaction model, indicating that cyber intrusion behavior is solely dictated by personality traits that act as dispositional tendencies that shape decision-making towards specific behavioral patterns, which are further influenced by situational factors, technical skills, and developmental aspects. The findings endorse the concept of dynamic cyber-personality profiles that develop through interactions and context, emphasizing flexibility over rigid categories.

Future research could build on this by using clustering, latent profile analysis, or longitudinal studies to empirically explore whether specific cyber-personality types remain consistent across various contexts and populations. The findings suggest that personality-based profiling works best when treated as probabilistic and context-dependent, rather than deterministic.

Comparison to Prior Research

This study's findings both support and extend existing research on the psychological aspects of cyber behavior. As in previous studies linking personality traits to cybersecurity decisions (e.g., Gaia et al., 2021; Maasberg et al., 2015), the results reaffirm that personal differences significantly influence how individuals respond to intrusions, beyond technical factors.

In particular, the strong link between the Dark Triad traits and behaviors such as persistence, deception, and risk-taking aligns with prior research identifying socially aversive traits as predictors of exploitative and rule-breaking actions in digital environments (Jones & Paulhus, 2014; Maasberg et al., 2015). The role of Psychopathy in repeated intrusion attempts reflects earlier findings linking emotional detachment and fearlessness to persistence under threat. Similarly, Machiavellianism's association with deception and manipulation aligns with established models of strategic Social Engineering (Jones & Paulhus, 2014; Maasberg et al., 2015).

The present study extends this literature by integrating the Big Five personality traits into a unified framework, demonstrating how normative traits regulate the expression of darker motivational tendencies. Findings on Conscientiousness and Openness align with prior research linking these traits to planning, creativity, and adaptive problem-solving (Costa & McCrae, 1992; McCrae & Costa, 1997), and further show that these traits shape style rather than intent alone.

Methodologically, this research enhances the existing literature by integrating quantitative modeling with qualitative reasoning, aligned with the MITRE ATT&CK Framework (MITRE, 2026). This method advances previous studies by connecting psychological traits to behavioral outcomes, tactical sequences, and decision-making processes (Gaia et al., 2022; Rege, 2013). Additionally, incorporating demographic moderators improves current models by illustrating how experience and development influence personality expression during cyber intrusions.

Overall, the findings support and extend existing research in cybersecurity and behavioral science by showing that intrusion behaviors arise from the interplay of dispositional traits,

cognitive regulation, and situational context. This synthesis reinforces the value of personality-informed models while highlighting the additional insights gained through mixed-methods and behavioral mapping approaches.

Practical Implications for Cybersecurity Defenses

The intrusion behaviors described by participants closely aligned with the stages outlined in the MITRE ATT&CK Framework, particularly reconnaissance, resource gathering, and initial access. These early phases emphasized how information is gathered, how the target's technical or physical environment is understood, and how preparation is carried out. Participants frequently described deliberate pre-planning, careful target assessment, and a phased decision-making process before advancing to more technically advanced intrusion behaviors. The narratives supported the quantitative findings, linking Conscientiousness to structured behaviors and reconnaissance actions, and highlighting how personality traits shape preparatory behaviors that can increase the likelihood of successful intrusions and attacks.

Participant responses also indicated that intrusion processes are rarely seen as a straightforward sequence of steps. Instead of moving smoothly through each phase, individuals described a fluid, adaptable decision-making process, often returning to earlier stages when encountering resistance or the risk of detection. Participants said that if there's a chance of detection, they would pause, erase traces, and switch to passive information-gathering until they find an opportunity to resume. This iterative pattern shows how intrusion behaviors adapt dynamically to environmental feedback rather than strictly adhering to a fixed set of procedures.

From a defensive perspective, these findings underscore the importance of adaptive, behaviorally informed detection strategies. No single tactic, technique, or procedure should be considered in isolation. Instead, defenders must examine patterns of behavior over time,

recognizing that attackers may shift tactics, retreat, or blend in, depending on opportunity and perceived risk. Detection and response strategies that rely solely on discrete Indicators of Compromise (IoCs) may miss the broader behavioral logic that guides adversary decision-making.

The structured and reconnaissance-oriented behaviors observed in the qualitative data also revealed that intrusion strategies are not purely technical acts but are shaped by underlying personality-driven preferences for order, control, and mastery. These behaviors frequently co-occurred with persistence and deception, underscoring the need to view attacker behavior holistically. Technically proficient individuals may simultaneously exhibit adaptive, manipulative, or psychologically strategic approaches, reflecting an interplay among skill, motivation, and disposition.

The findings offer exploratory insights relevant to cybersecurity practice, workforce development, and defensive planning. The integration of quantitative and qualitative reasoning demonstrates that intrusion behavior is not driven solely by technical capabilities. Individual differences in personality, motivation, and emotional regulation influence how technical knowledge is applied, adapted, and sustained during intrusion activity. Recognizing these differences may help organizations better understand behavioral variability among both adversaries and defenders.

The findings indicate that cybersecurity performance results from an interaction between motivational and regulatory traits. Although technical certifications and training are crucial, the study suggests that enhancing training and professional development with a focus on self-awareness, ethical decision-making, and behavioral regulation could be advantageous.

An understanding of cognitive styles and personality traits may help organizations design cybersecurity operational roles and responsibilities. For example, those high in Conscientiousness and Openness may be well suited for roles involving threat hunting, detection engineering, or architectural design, where they can leverage their preference for procedural discipline alongside creative problem-solving. Those higher in Extraversion and lower in Agreeableness may excel in roles such as penetration testing or red teaming, where assertive and persuasive behaviors are necessary.

The findings emphasize the need to include ethics and self-regulation in cybersecurity education explicitly. Traits like Machiavellianism and Psychopathy, associated with persistence, strategic manipulation, and risk tolerance, were connected to ongoing, high-risk behaviors during the simulated intrusion. Although these traits do not necessarily indicate malicious intent, they could lead to boundary-pushing actions if not managed by professional norms. Mentorship, scenario-based ethics training, and organizational accountability can help steer these high-risk cognitive traits toward positive, security-oriented outcomes.

From a threat intelligence perspective, this research offers a complementary behavioral lens for understanding attacker activity. MITRE ATT&CK provides a robust taxonomy of observable TTPs, but it does not explain why a particular individual or threat actor group may favor a specific strategy. The current findings suggest that personality-driven factors, such as dominance orientation, strategic deception, and emotional detachment, may influence the selection, sequencing, and persistence of TTPs. Incorporating behavioral insights alongside technical indicators may enhance attribution, prioritization, and threat anticipation without replacing existing analytical frameworks.

Importantly, personality traits did not map neatly onto individual TTPs. Instead, individual differences spanned multiple tactics and phases simultaneously, reflecting the hybrid and adaptive nature of intrusion decision-making. The findings reinforce that cyber intrusions are not linear technical scripts but rather evolving processes shaped by motives, skills, and situational opportunity. The psychological perspective, therefore, complements but does not replace the MITRE ATT&CK Framework's technical focus by providing insights into intent, flexibility, and behavioral logic.

The findings support a wider move towards human-centered cybersecurity defense strategies. Social Engineering proved to be the most common tactic, highlighting that human vulnerabilities are key to successful intrusions. Training programs that focus solely on technical controls could be improved by incorporating behavioral science concepts such as trust, persuasion, cognitive bias, and emotional influence. Knowing why manipulation works is just as vital as recognizing how it happens.

Taken together, the practical implications of this study should be viewed as exploratory and foundational. Further empirical research is needed to assess whether personality-informed approaches meaningfully improve training outcomes, defensive effectiveness, or risk mitigation in applied environments. Nonetheless, the results underscore a critical insight that effective cybersecurity cannot rely on technology alone. Cyber intrusions reflect human decision-making, which is shaped by personality, motivation, and context. Integrating behavioral science with technical frameworks offers a promising direction for advancing research and practice in cybersecurity.

Limitations

While the current study offers valuable insights into the relationship between personality traits and decisions about cyber intrusions, several limitations must be acknowledged. These limitations do not diminish the study's contribution but provide important context for interpreting the findings and identifying directions for future work.

First, the study employed a tabletop exercise (TTX) design in which participants were asked to describe how they would respond to a simulated cyber intrusion scenario, rather than observing real-world behavior. As a result, the findings reflect hypothetical decision-making, intentions, and cognitive reasoning, rather than verified operational actions. Participants' responses may not align with how they would behave under real-world conditions involving legal risk, time pressure, uncertainty, or consequences. This limitation is inherent to scenario-based research and means that the findings should be interpreted as indicators of behavioral preferences and reasoning patterns rather than direct predictors of actual intrusion behavior.

Relatedly, the TTX format captures what participants believe is an appropriate or effective approach, as ceded by professional norms, training, or retrospective rationalization. Some participants may describe idealized or socially acceptable strategies rather than those they would realistically execute in practice. However, the exercise remains a preferred method for studying cognitive styles, threat modeling, and adaptation without exposing participants or systems to harm. The strength of this approach is its ability to reveal how individuals conceptualize problems, prioritize actions, and justify decisions, even if real-world execution may vary.

Secondly, the study relied on a self-selected convenience sample of 257 participants, of whom 196 completed the full survey, including the open-ended components. While this is a substantial sample for a mixed-methods design, it cannot be assumed to represent the broader

population of cyber threat actors. Recruitment through platforms such as Reddit and Discord likely introduced selection bias toward individuals with legitimate cybersecurity or penetration testing experience, while underrepresenting those actively engaged in illicit or covert hacking activities. Consequently, generalizations to the full spectrum of cyber threat actors, particularly those engaged in highly illegal or state-sponsored activities, should be approached cautiously.

Third, personality traits were measured using self-report instruments, which are vulnerable to socially desirable responding and self-presentation effects, especially when assessing socially aversive traits such as Machiavellianism and Psychopathy. Although participants' anonymity may have reduced response distortion, it remains possible that some individuals underreport or exaggerate certain traits. Similarly, open-ended responses reflect self-described reasoning rather than externally validated behavior.

Fourth, although qualitative coding followed established reliability standards (Landis & Koch, 1977) and achieved very high inter-rater agreement ($\kappa = 0.98$), interpretation bias remains an inherent limitation of content analysis. Mapping free-text responses to behavioral categories and MITRE ATT&CK phases required subjective judgment, particularly when responses were brief, ambiguous, or described multi-phased strategies. Additionally, binary coding facilitated statistical analysis but necessarily reduced complex, iterative intrusion processes into simplified categories, potentially obscuring nuance and sequence.

Finally, while the MITRE ATT&CK Framework provides a rigorous, standardized taxonomy for categorizing technical behaviors, it is not designed to capture psychological motivation or intent. Many participant responses spanned multiple phases or reflected blended tactics that did not map clearly onto discrete TTPs, underscoring the limitations of applying a technically oriented framework to cognitively driven narratives.

In sum, this study prioritizes internal consistency, theoretical integration, and methodological transparency while acknowledging the trade-offs inherent in scenario-based and self-report research. The findings should be viewed as exploratory yet foundational, offering empirically grounded insights into how personality traits shape intrusion reasoning, preferences, and strategic orientation. Future research incorporating observational methods, longitudinal designs, red-teaming simulations, or real-world behavioral telemetry would further strengthen understanding of how these cognitive patterns translate into operational behavior.

Future Research

Building on the current study's findings and limitations, several suggestions for future research are offered. These emphasize refining methodologies and broadening theoretical frameworks to better understand personality-driven cyber intrusion behaviors and to create more effective tools for cybersecurity professionals.

Future research should broaden data collection beyond self-identified cybersecurity professionals and hackers to include the full spectrum of adversarial behavior, including gray and black-hat hackers. Although this group can be difficult to access, partnering with law enforcement or attending targeted events like DefCon or BlackHat conferences may help gather a more diverse sample. This strategy can help determine whether the patterns found in the study are relevant across different motivational and moral backgrounds.

This study relied on self-reports and hypothetical decisions in a simulated scenario. Future research should incorporate direct behavioral observations, controlled experiments, or virtual intrusion simulations to directly assess the technical choices individuals make. Research could also collect firsthand insights from those involved in cyber intrusions. Post-conviction interviews with offenders might provide valuable insight into real-world decision-making. This

approach would extend beyond simulations and examine how psychological traits manifest in real situations.

In summary, the current study lays a foundation for a more psychologically informed understanding of cyber intrusion behaviors. Future research should broaden the sample population and enhance behavioral realism. By refining the link between personality, behavior, and cybersecurity, scholars can move closer to predicting, mitigating, and ultimately preventing malicious and risky cyber intrusions through a deeper understanding of the human factors that drive these behaviors.

CONCLUSION

The study examined how personality traits in the Big Five and the Dark Triad influence decision-making about cyber intrusions. Using a mixed-methods design that combined quantitative modeling with qualitative analysis of participants' reasoning, the study sought to understand how dispositions shape tactical choices in a simulated cyber intrusion scenario. By integrating psychological theory with cybersecurity practice, the work contributes to a growing body of literature that places human behavior at the center of cybersecurity.

Across the analytic approaches, the findings showed that personality exerts a subtle but measurable influence on intrusion decision-making. Dark personality traits, particularly Psychopathy and Machiavellianism, emerged as consistent predictors of bold, persistent, and deceptive behaviors. These traits were associated with goal-oriented focus, emotional detachment, and strategic manipulation, suggesting that high-risk intrusion behaviors are often driven by calculated opportunity rather than impulsivity alone. Psychopathy was most strongly linked to persistence in the face of deterrence, while Machiavellianism predicted deception and controlled risk-taking, reflecting deliberate and strategic decision-making processes.

The Big Five traits, while less predictive, added meaningful nuance to understanding behavioral variability, procedural styles, and motivational intensity. Conscientiousness aligned with structured, sophisticated approaches. These individuals used systematic, organized methods, reflecting precision and planning. Openness corresponded with creative, exploratory strategies, emphasizing flexibility and adaptability. Extraversion contributed to assertive, socially engaged intrusion reasoning, particularly in behaviors that involved confidence and initiative. Together, these findings reinforce that technical outcomes in cyber intrusion scenarios are influenced not

only by skill but also by how individuals perceive risk, manage uncertainty, and structure their problem-solving approaches.

Demographic moderators added important context to the interpretation of personality-related decision-making in the simulated intrusion scenario. Age moderated the relationship between Psychopathy and persistence, with younger participants more likely to endorse continued intrusion efforts and older participants showing greater restraint. Cybersecurity involvement also enhanced the predictive accuracy of structured and sophisticated intrusion strategies, suggesting that technical experience shapes how personality traits are expressed in reasoning about intrusion tactics. Rather than indicating deterministic behavioral outcomes, these results imply that expertise may amplify or constrain personality-driven tendencies by providing individuals with learned frameworks, tools, and procedural knowledge to draw upon when conceptualizing an intrusion.

Taken together, the findings reinforce that personality traits do not operate in isolation but interact with life phases and professional experience, which influence how individuals conceptualize and justify intrusion behaviors in a simulated context. This interaction underscores the importance of viewing cyber intrusion decision-making as a person-situation process, where dispositional traits, experience, and contextual demands jointly shape strategic thinking within the cyber environment.

The Random Forest validation strengthened the interpretations by demonstrating result stability. Personality and demographic variables jointly predicted intrusion styles, with accuracy ranging from 73 to 96%. Psychopathy and Machiavellianism consistently ranked as the most influential predictors, followed by Conscientiousness and Extraversion. This confirms that both impulsivity and organization are central components of attacker thinking. The cross-method

consistency reinforces the robustness of the study's core findings and underscores the value of combining traditional inferential statistics with modern machine-learning techniques in behavioral Cybersecurity research.

The qualitative analyses provided a rich understanding of the patterns. The analysis revealed why individuals make certain decisions. Participants described adaptive, multi-layered reasoning that mirrored real-world adversarial behavior. The narratives confirmed that intrusion behavior rarely occurs in isolation. Rather, the intrusion methods are dynamic and highly context-dependent. The participants' explanations echoed the quantitative findings that intrusions are shaped by a myriad of variables, with personality providing the underlying foundation.

The study made several contributions to theoretical frameworks. It extends personality-behavior research into the cybersecurity domain, providing empirical evidence that distinct personality profiles influence technical decision-making. It also supports using the Big Five and the Dark Triad as complementary lenses to explain cyber intrusion behaviors. These insights can help improve cybersecurity training, threat detection, and proactive defenses by revealing the psychological mechanisms underlying intrusion behaviors.

Although exploratory in nature, the findings offer several implications for cybersecurity practice. They suggest that human-centric considerations may complement technical controls in training, workforce development, and defensive strategy design. Awareness of dispositional tendencies related to persistence, deception, and risk tolerance may inform ethical training, insider threat awareness programs, and role-specific supervision frameworks. Importantly, these findings do not imply a deterministic use of personality traits but highlight the value of understanding how individual differences may influence behavior under pressure.

In the educational context, the results support integrating behavioral science concepts into cybersecurity curricula. Emphasizing self-awareness, ethical reasoning, and cognitive diversity alongside technical instruction may help prepare professionals to recognize both adversarial behavioral patterns and their own decision-making tendencies in high-stakes environments.

Several avenues for future research emerged from this work. Longitudinal studies are needed to examine whether personality-driven intrusion tendencies remain stable over time or change with experience, training, emerging technologies, and ethical development. Cross-cultural replication could assess how cultural norms and institutional contexts influence the expression of personality traits in cyber intrusion decision-making. Additionally, future research may explore integrating personality-informed behavioral patterns with machine-learning-based threat profiling to enhance the interpretability and contextual understanding of predictive models.

Ultimately, the research reinforces that cybersecurity and cyber threats are not only technical but also human-centric. The same cognitive processes that govern social interaction also guide how individuals approach the execution of cyber-attacks. Understanding these processes through the lens of personality enables nuanced defensive strategies, ethical offensive training, and a deeper understanding of the human element in cyber vulnerabilities.

In conclusion, combining personality insights with cybersecurity greatly improves our understanding of the threat environment. Linking individual traits to operational actions helps explain how personality affects security breaches. Future studies should further blend quantitative methods with qualitative insights.

Through the work in the current study, cybersecurity is reframed as a human ecosystem where psychology and technology converge. Understanding the dispositional foundations of

intrusion behavior provides new opportunities for prediction, prevention, and education. It empowers defenders to anticipate adversaries from a logical perspective.

The study's broader implication is clear: as technology continues to evolve, so does our understanding of the human minds that drive it. By viewing cybersecurity through a behavioral lens, researchers and practitioners can move beyond reactive defense to proactive insights. This research, therefore, stands both as a conclusion and as a beginning, a foundation for future understanding of the human element in cybersecurity, where interdisciplinary collaboration is necessary to secure the systems that modern society depends on.

Overall, this study reinforced the view that cybersecurity is not solely a technical domain but a human ecosystem shaped by cognition, motivation, and experience. By empirically linking personality traits to intrusion reasoning, the research advances understanding of how individual differences shape the structure and intent of cyber intrusion behaviors. Although not predictive or prescriptive, the findings lay a foundation for interdisciplinary inquiry into the psychological dimensions of cybersecurity.

As cyber threats continue to evolve, understanding the human minds behind them is increasingly important. Viewing cybersecurity through a behavioral lens enables more nuanced defensive thinking, ethically grounded training, and deeper insight into adversarial decision-making. The study therefore serves as both a conclusion and a starting point for future research at the intersection of psychology and cybersecurity.

REFERENCES

Abbasi, A., Li, W., Benjamin, V., Hu, S., & Chen, H. (2014). Descriptive analytics: examining expert hackers in web forums. *2014 IEEE Joint Intelligence and Security Informatics Conference*. https://doi.org/10.1109/jisic.2014.18

Abbott, S. (2019). Improving insider threat training awareness and mitigation programs at nuclear facilities. *Project on Nuclear Issues: A Collection of Papers from the 2017 Conference Series and Nuclear Scholars Initiatives.* https://doi.org/10.2172/1367469.

Achor, S. Z., Zaria, L. I., & Achor, E. E. (2022). Perceived cognitive load and students' performance in social studies. *Journal of Research in Instructional, 2(2)*, 129-140. https://doi.org/10.30862/jri.v2i2.74

Ahmad, S., Urus, S., & Nazri, S. (2021). Technology acceptance of financial technology (fintech) for payment services among employed fresh graduates. *Asia-Pacific Management Accounting Journal, 16(2),* 27-58. https://doi.org/10.24191/apmaj.v16i2-02

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2019). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953. https://doi.org/10.1002/asi.24311.

Ahmed, M., Panda, S., Xenakis, C., & Panaousis, E. (2022). MITRE ATT&CK-driven cyber risk assessment. P*roceedings of the 17th International Conference on Availability, Reliability and Security.* https://doi.org/10.1145/3538969.3544420

Ahmed, I., & Islam, T. (2022). Dark personality triad and cyber entrepreneurial intentions: The mediation of cyber entrepreneurial self-efficacy and moderation of positive thinking. *Kybernetes*, *52*(9), 3022-3043. https://doi.org/10.1108/k-05-2022-0765.

Akdemir, N., & Yenal, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open*, *11*(3), 215824402110318-. https://doi.org/10.1177/21582440211031879

Albladi, S. M. & George, R. S. (2017). Personality traits and cyber-attack victimisation: multiple mediation analysis. *2017 Internet of Things Business Models, Users, and Networks.* https://doi.org/10.1109/ctte.2017.8260932

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of Social Engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1). https://doi.org/10.1186/s13673-018-0128-7

Allemand, M., Gomez, V., & Jackson, J. J. (2010). Personality trait development in midlife: exploring the impact of psychological turning points. *European Journal of Ageing, 7*(3), 147-155. https://doi.org/10.1007/s10433-010-0158-0

Allman, T. (2018). Understanding Personality. *ReferencePoint Press.*

Allport, G. W., & Odbert, H. S. (1936). Trait names: A psycho-lexical, study. *Psychological Monographs,* 47(1, Whole No. 211)

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information and Computer Security*, *26*(3), 306–326. https://doi.org/10.1108/ICS-03-2018-0037.

Al-Shaer, R.; Spring, J.M.; Christou, E. (2022). Learning the Associations of MITRE ATT&CK Adversarial Techniques. *In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS)*.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531-. https://doi.org/10.1016/j.chb.2020.106531

American Psychological Association (2025). Personality. Retrieved from: https://www.apa.org/topics/personality

Amo, L., Gaia, J., Murray, D., Sanders, G. L., Sanders, S. P., Upadhyaya, S., & Wang, X. (2023). Primary and secondary control as antecedents to the dark traits in predicting attraction to hacking behavior. *Journal of Organizational Psychology, 23*(3). https://doi.org/10.33423/jop.v23i3.6488

Angeles, R., Dolovich, L., Kaczorowski, J., & Thabane, L. (2013). Developing a theoretical framework for complex community-based interventions. *Health Promotion Practice, 15(1),* 100-108. https://doi.org/10.1177/1524839913483469

Anwar, M. (2015). Mixed-methods research in pharmacy practice and its implications. *Archives of Pharmacy Practice, 6(1),* 1. https://doi.org/10.4103/2045-080x.151279

Ashton, M. (2023). Chapter 3 – Personality Structure Classifying Traits. *Individual Differences and Personality. 4.* https://doi.org/10.1016/B978-0-323-85950-9.00005-4

Babcock, S. E., & Wilson, C. A. (2020). Big five model of personality. In *The Wiley Encyclopedia of Personality and Individual Differences: Personality Processes and Individual Differences, Volume III, First Edition* (Vol. 3).

Back, M. D., Schmukle, S. C., & Egloff, B. (2010). Why are narcissists so charming at first sight? Decoding the narcissism–popularity link at zero acquaintance. *Journal of Personality and Social Psychology, 98*(1), 132–145.

Bada, M., & Nurse, J. R. (2021). Profiling the Cybercriminal: A systematic review of research. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. https://doi.org/10.1109/cybersa52016.2021.9478246

Bada, M., & Nurse, J. R. (2023). Exploring Cybercriminal activities, behaviors, and profiles. *Applied Cognitive Science and Technology*, 109-120.

Bajwa, M. J. & Khalid, R. (2015). Impact of personality on vengeance and forgiveness in young adults. *Journal of Psychology &Amp; Clinical Psychiatry, 2*(5). https://doi.org/10.15406/jpcpy.2015.02.00088

Bakas, A., Wagner, A., Johnston, S., Kennison, S., & Chan-Tin, E. (2021). Impact of personality types and matching messaging on password strength. *EAI Endorsed Transactions on Security and Safety*, *8*(28). https://doi.org/10.4108/eai.1-6-2021.170012

Bakelants, H., Vanderstichelen, S., Chambaere, K., Droogenbroeck, F., Donder, L., Deliens, L., Dury, S., & Cohen, J. (2022). Researching compassionate communities: Identifying theoretical frameworks to evaluate the complex processes behind public health palliative care initiatives. *Palliative Medicine, 37(2),* 291-301. https://doi.org/10.1177/02692163221146589

Banda, R., Phiri, J., Nyirenda, M., & Kabemba, M. M. (2019). Technological paradox of hackers begetting hackers: a case of ethical and unethical hackers and their subtle tools. *Zambia ICT Journal, 3*(1), 40-51. https://doi.org/10.33260/zictjournal.v3i1.74

Baranski, E. N., Morse, P. J., & Dunlop, W. L. (2017). Lay conceptions of volitional personality change: From strategies pursued to stories told. *Journal of Personality*, *85*(3), 285–299. https://doi.org/10.1111/jopy.12240

Basak, A., Černý, J., Gutierrez, M., Curtis, S. R., Kamhoua, C. A., Jones, D. N., Bošanský, B., & Kiekintveld, C. (2018). An initial study of targeted personality models in the flipit game. *Lecture Notes in Computer Science*, 623-636. https://doi.org/10.1007/978-3-030-01554-1_36

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers &Amp; Security, 65*, 153-165. https://doi.org/10.1016/j.cose.2016.10.007

Bates, T. C. (2023). Signaling virtuous Victimhood as indicators of dark triad personalities: A replication and extension of OK et al (2021). https://doi.org/10.31234/osf.io/cqj6h

Belfadel, A., Boyer, M., Letailleur, J., Petiot, Y., & Yaich, M., (2022). Towards a security impact analysis framework: A risk-based and MITRE Attack approach. *27th European Symposium on Research in Computer Sciences.*

Belmont Report. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.

Benjamin, V., Li, W., Holt, T. J., & Chen, H. (2015). Exploring threats and vulnerabilities in hacker web: forums, IRC, and carding shops. *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*. https://doi.org/10.1109/isi.2015.7165944

Benjamin, V., Valacich, J. S., & Chen, H. (2019). Dice-e: a framework for conducting darknet identification, collection, and evaluation with ethics. *MIS Quarterly, 43(1),* 1-22. https://doi.org/10.25300/misq/2019/13808

Bergner, R. (2020). What is personality? Two myths and a definition. *New Ideas in Psychology, 57.* https://doi.org/10.1016/j.newideapsych.2019.100759

Berndt, A. and Ophoff, J. (2020). Exploring the value of a cyber threat intelligence function in an organization. Information Security Education. *Information Security in Action,* 96-109. https://doi.org/10.1007/978-3-030-59291-2_7

Bernerth, J. B., Aguinis, H., & Taylor, E. C. (2021). Detecting false identities: a solution to improve web-based surveys and research on leadership and health/well-being. *Journal of Occupational Health Psychology, 26*(6), 564-581. https://doi.org/10.1037/ocp0000281

Bhogal, M. and Wallace, D. (2021). Cost-inflicting mate retention tactics predict the perpetration of cyber dating abuse. *Evolutionary Psychological Science, 8*(1), 1-9. https://doi.org/10.1007/s40806-021-00307-8

Black, M. (2022). Insider threat and white-collar crime in non-government organisations and industries: A literature review. https://doi.org/10.7249/rra1507-1

Bolelli, M. (2020). The effects of dark triad (Machiavellianism, narcissism, psychopathy) on the love attitudes. *JOURNAL OF CURRENT DEBATES IN SOCIAL SCIENCES*, *2*(2), 164-173. https://doi.org/10.37154/ijopec.2019.3

Book, A., Methot, T., Gauthier, N., Hosker-Field, A., Forth, A., Quinsey, V., & Molnar. (2015). The mask of sanity revisited: Psychopathic traits and affective mimicry. *Evolutionary Psychological Science, 1*(2), 91–102. http://dx.doi.org/10.1007/s40806-015-0012-x.

Brainard, J., Houghton, J., Bunn, D., Watts, L., Mumford, S., O'Brien, S., & Lane, K. L. (2022). The wasps are clever: keeping out and finding bot answers in internet surveys used for health research. *Preprint.* https://doi.org/10.20944/preprints202203.0243.v2

Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32.

Buchanan, T., & Whitty, M. T. (2014). The online disinhibition effect: Personality and deceptive self-presentation on social networking sites. *Frontiers in Psychology, 5*, 1–10. https://doi.org/10.3389/fpsyg.2014.00539

Buckels, E. E., Jones, D. N., & Paulhus, D. L. (2013). Behavioral confirmation of everyday sadism. *Psychological Science, 24*(11), 2201 - 2209. https://doi.org/10.1177/0956797613490749

Budimir, S., et al., (2021). Emotional Experiences of Cyber-security Breach Victims. *Cyberpsychology, Behavior and Social Networking, 2(9).*

Burruss, G. W., Howell, C. J., Maimon, D., & Wang, F. (2021). Website defacer classification: a finite mixture model approach. *Social Science Computer Review, 40(3),* 775–787. https://doi.org/10.1177/0894439321994232

Burton, S., (2023). Cybersecurity Risk: The business significance of ongoing tracking. *Transformational Interventions for Business, Technology, and Healthcare.*

Busuioc, A. & Butucescu, A. (2020). The role of dark triad on the link between emotional labor and core burnout. *Psihologia Resurselor Umane, 18*(1), 51-64. https://doi.org/10.24837/pru.v18i1.461

Cai, J., Xu, Z., Sun, X., Xiao-jun, G., & Fu, X. (2023). Validity and reliability of the Chinese version of threats of artificial intelligence scale (tai) in Chinese adults. *Psicologia: Reflexão E Crítica, 36*(1). https://doi.org/10.1186/s41155-023-00247-1

Carton, H., & Egan, V. (2017). The dark triad and intimate partner violence. *Personality and Individual Differences, 105*, 84-88.

Carvalho, L. de F., Pianowski, G., & Gonçalves, A. P. (2020). Personality differences and COVID-19: are extroversion and Conscientiousness personality traits associated with engagement with containment measures? *Trends in psychiatry and psychotherapy*.

Ceccato, M., Tonella, P., Basile, C., Coppens, B., Sutter, B. D., Falcarin, P., … & Torchiano, M. (2017). How professional hackers understand protected code while performing attack tasks. *2017 IEEE/ACM 25th International Conference on Program Comprehension (ICPC)*. https://doi.org/10.1109/icpc.2017.2

Chen, H., Cohen, P., & Chen, S. (2010). How big is a big odds ratio? Interpreting the magnitude of odds rations in epidemiological studies. *Communications in Statistics – Simulation and Computation, 39*(4), 860-864. https://doi.org/10:1080/03610911003650383

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167-. https://doi.org/10.1016/j.chbr.2022.100167

Cho, J.-H., Cam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016*, 7–13.

Christen, P., Ranbaduge, T., & Schnell, R. (2020). *Linking sensitive data : methods and techniques for practical privacy-preserving information sharing* (1st ed. 2020.). Springer. https://doi.org/10.1007/978-3-030-59706-1

Christie, R., & Geis, F. L. (2013). *Studies in Machiavellianism*. *Academic Press*.

Cobb-Clark, D. A. & Schurer, S. (2011). The stability of big-five personality traits. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.1922015

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. *Routledge*. https://doi.org/10.4324/9780203771587

Čopková, R. & Christenková, Z. (2021). The effect of dark triad traits on decision-making styles. *Psychological Thought, 14*(1), 74-93. https://doi.org/10.37708/psyct.v14i1.556

Costa Jr, P. T., McCrae, R. R., & Dye, D. A. (1991). Facet scales for Agreeableness and Conscientiousness: A revision of the NEO Personality Inventory. *Personality and Individual Differences, 12*(9), 887-898.

Costa, P. T., Jr., & McCrae, R. R. (1992). *Revised NEO Personality Inventory (NEO PI-R) and NEO Five-Factor Inventory (NEO-FFI) professional manual.* Psychological Assessment Resources.

Coutinho, J., Sampaio, A., Ferreira, M., Soares, J. M., & Gonçalves, Ó. F. (2013). Brain correlates of pro-social personality traits: a voxel-based morphometry study. *Brain Imaging and Behavior, 7*(3), 293-299. https://doi.org/10.1007/s11682-013-9227-2

Credé, M., Harms, P. D., Niehorster, S., & Gaye-Valentine, A. (2012). An evaluation of the consequences of using short measures of the big five personality traits. *Management Department Faculty Publications*. https://digitalcommons.unl.edu/managementfacpub/86

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

CrowdStrike (2023). *2023 Global Threat Report*. Retrieved from: https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf

CrowdStrike (2024). 2024 Global Threat Report. Retrieved from: *https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf*

CrowdStrike (2025). *2025 Global Threat Report*. Retrieved from: https://www.crowdstrike.com/en-us/global-threat-report/

Curtis, S. R., Basak, A., Carré, J., Bošanský, B., Černý, J., Ben-Asher, N., Gutierrez, M., Jones, D. N., & Kiekintveld, C. (2021). The dark triad and strategic resource control in a competitive computer game. *Personality and Individual Differences, 168,* 110343. https://doi.org/10.1016/j.paid.2020.110343

Curtis, S. R., Rajivan, P., Jones, D. N., & González, C. (2018). Phishing attempts among the dark triad: patterns of attack and vulnerability. *Computers in Human Behavior, 87,* 174-182. https://doi.org/10.1016/j.chb.2018.05.037

Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to Social Engineering attacks. *Australian Information Security Management Conference*.

Dang, F., Yan, L., Wu, K., & Li, D. (2023). Research on deceptive dynamic defense method based on sdn. *Sixth International Conference on Computer Information Science and Application Technology (CISAT 2023).* https://doi.org/10.1117/12.3004599

De Paoli, S., & Johnstone, J. (2023). A qualitative study of penetration testers and what they can tell us about information security in organisations. *Information Technology & People*. https://doi.org/10.1108/itp-11-2021-0864

Deepwatch, (2024). ATI 2024 Annual Threat Report.

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747.

Ding, Z., Benjamin, V., Liu, W., & Yin, X. (2021). Exploring differences among darknet and surface internet hacking communities. *2021 IEEE International Conference on Intelligence and Security Informatics (ISI).* https://doi.org/10.1109/isi53945.2021.9624681

Drawve, G., Thomas, S. A., & Hart, T. C. (2017). Routine activity theory and the likelihood of arrest: a replication and extension with conjunctive methods. *Journal of Contemporary Criminal Justice, 33(2),* 121–132. https://doi.org/10.1177/1043986216689747

DTEX i3, (2023). 2023 Insider Risk Investigations Report. The Rise of Employee Attrition and Data Exfiltration. Retrieved from: *https://www2.dtexsystems.com/l/464342/2023-03-16/3p3ytt/464342/16789745276zZiMsd3/DTEX_Report_2023InsiderRiskInvestigationsReport.pdf*

Dupuis, M., & Gleason, N. (2020). An examination of personality and individual differences in cybersecurity professionals. *Frontiers in Psychology, 11*, 568506. https://doi.org/10.3389/fpsyg.2020.568506

Dyce, J. A. (1997). The big five factors of personality and their relationship to personality disorders. *Journal of Clinical Psychology*, *53*(6), 587–593.

EarthWeb. (n.d.). Retrieved from earthweb.com.

Ekvall, K. O. & Molstad, A. J. (2022). Mixed-type multivariate response regression with covariance estimation. *Statistics in Medicine, 41(15),* 2768-2785. https://doi.org/10.1002/sim.9383

Ellen, B., Alexander, K., Mackey, J., McAllister, C., & Carson, J. (2021). Portrait of a workplace deviant: a clearer picture of the Big Five and Dark Triad as predictors of workplace deviance. *Journal of Applied Psychology, 106*(12), 1950-1961. https://doi.org/10.1037/apl0000880f

Eronen, M. I. & Romeijn, J. (2020). Philosophy of science and the formalization of psychological theory. *Theory &Amp; Psychology, 30*(6), 786-799. https://doi.org/10.1177/0959354320969876

Еропова, M. (2019). Factor structure of the short dark triad (sd3) in adolescents. *The European Proceedings of Social and Behavioural Sciences.* https://doi.org/10.15405/epsbs.2019.07.17

eSentire, (2023). Cybercrime to Cost the World $9.5 Trillion USD Annually in 2024.

Fagade, T., et al., (2017). System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis. *The Human Aspects of Information Security, Privacy and Trust*, 5.

Fagade, T., Tryfonas, T., & Crick, T. (2019). Exploring personality traits for effective cyber security analysts. *Information & Computer Security, 27*(2), 157–175. https://doi.org/10.1108/ICS-06-2018-0075

Falowo, O., Popoola, S., Riep, J., Adewopo, V., & Koch, J. (2022). Threat Actors' Tenacity to disrupt: Examination of major cyberseucrity incidents. *IEEE, 10,* 134038. doi: 10.1109/ACCESS.2022.3231847

Farhadi, H., Omar, F., Nasir, R., & Shahrazad, W. (2012). Agreeableness and Conscientiousness as antecedents of deviant behavior in workplace. *Asian Social Science, 8*(9). https://doi.org/10.5539/ass.v8n9p2

FBI IC3, (2023). Federal Bureau of Investigations Internet crime report 2022. Retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Filiol, E., Mercaldo, F., & Santone, A. (2021). A method for automatic penetration testing and mitigation: A red hat approach. *Procedia Computer Science*, *192*, 2039-2046. https://doi.org/10.1016/j.procs.2021.08.210

Fleck, A., (2024). Cybercrime expected to skyrocket in coming years. *Statista.* Retrieved from: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Foster, S., & Cross, J. (2024). Dark doxxing: How dark triad traits impact support for doxxing behaviors. *Personality and Individual Differences*, *217*, 112432. https://doi.org/10.1016/j.paid.2023.112432

Fox, J., (2023). Top cybersecurity statistics for 2024. *Cobalt.io.* Retrieved from: https://www.cobalt.io/blog/cybersecurity-statistics-2024

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

Furnell, S., Shah, J. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud & Security, 8*. https://doi.org/10.1016/S1361-3723(20)30084-1

Furnham, A., & Cuppello, S. (2024). Correlates of the Dark Tetrad. *Acta psychologica*, *245*, 104222. https://doi.org/10.1016/j.actpsy.2024.104222

Furnham, A., Richards, S. C., & Paulhus, D. L. (2013). The dark triad of personality: A 10 Year review. *Social and Personality Psychology Compass*, *7*(3), 199-216. https://doi.org/10.1111/spc3.12018

Gaia, J., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. (2021). Dark Traits and Hacking Potential. *Journal of Organizational Psychology*, *21*(3). https://doi.org/10.33423/jop.v21i3.4307

Gaia, J., Murray, D., Sanders, G., Sanders, S., Upadhyaya, S., Wang, X., & Yoo, C. (2022). The interaction of dark traits with the perceptions of apprehension. *Proceedings of the Annual Hawaii International Conference on System. Sciences*. https://doi.org/10.24251/hicss.2022.279

Gaia, J., Ramamurthy, B., Sanders, G., Sanders, S., Upadhyaya, S., Wang, X., & Yoo, C. (2020). Psychological profiling of hacking potential. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2020.273

Gaines, S., Jr. (2019). *CURRENT AND EMERGING SCHOOLS OF THOUGHT*. http://ebookcentral.proquest.com/lib/purdue/detail.action?docID=5928942

Gamachchi, A. & Boztaş, S. (2017). Insider threat detection through attributed graph clustering. *2017 IEEE Trustcom/BigDataSE/ICESS*. https://doi.org/10.1109/trustcom/bigdatase/icess.2017.227

Gammon, A., Converse, P., Lee, L., & Griffith, R. (2011). A personality process model of cyber harassment. *International Journal of Management and Decision Making, 11*(5/6), 358. https://doi.org/10.1504/ijmdm.2011.043409

Garcia, D. & Moraga, F. R. G. (2017). The dark cube: dark character profiles and ocean. *PeerJ, 5*, e3845. https://doi.org/10.7717/peerj.3845

Garcia, D., Adrianson, L., Archer, T., & Rosenberg, P. (2015). The Dark Side of the Affective Profiles: Differences and Similarities in Psychopathy, Machiavellianism, and Narcissism. *Sage Open*, *5*(4). https://doi.org/10.1177/2158244015615167

Geel, M. V., Goemans, A., Toprak, F., & Vedder, P. (2017). Which personality traits are related to traditional bullying and cyberbullying? A study with the big five, dark triad, and sadism. *Personality and Individual Differences, 106*, 231-235. https://doi.org/10.1016/j.paid.2016.10.063

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk Using a cyber-security culture framework. *Sensors, 21*(9), 3267.

Gerber, N., Gerber, N., & Hernando, M. (2017). Sharing the 'Real Me' – How Usage Motivation and Personality Relate to Privacy Protection Behavior on Facebook. *The Human Aspects of Information Security, Privacy and Trust, 5*.

Geukes, K., van Zalk, M., & Back, M. (2018). Understanding personality development: an integrative state process model. *International Journal of Behavioral Development, 42*(1), 43-51. https://doi.org/10.117/0165025416677847

Glazier, R. A., Boydstun, A. E., & Feezell, J. T. (2021). Self-coding: a method to assess semantic validity and bias when coding open-ended responses. *Research &Amp; Politics, 8*(3), 205316802110317. https://doi.org/10.1177/20531680211031752

Goasduff, L., (2023). Gartner Forecasts Global Security and Risk management spending to grow 14% in 2024, Public Cloud services growth to bolster cloud security spending. *Gartner.com*.

Goerzen, M. (2021). Wearing many hats. *AAAS Articles DO Group*. https://datasociety.net/wp-content/uploads/2022/03/WMH_final01062022Rev.pdf

Goldberg, L. R. (1990). An alternative "description of personality": The big-five factor structure. *Journal of Personality and Social Psychology*, *59*(6), 1216–1229.

Goldberg, L. R. (1993). The structure of phenotypic personality traits. *American Psychologist*, 48(1), 26–34. https://doi.org/10.1037/0003-066X.48.1.26

Gómez-Leal, R., Fernández-Berrocal, P., Gutiérrez-Cobo, M. J., et al. (2024). The Dark Tetrad: Analysis of profiles and relationship with the Big Five personality factors. *Scientific Reports*, *14*.

Gosling, S. D., Rentfrow, P. J., & Swann Jr., W. B. (2003). A very brief measure of the big-five personality domains. *Journal of Research in Personality*, *37*(5). https://doi.org/10.1016/S0092-6566(03)00046-1

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

Griffin, M., Martino, R. J., LoSchiavo, C., Comer-Carruthers, C., Krause, K. D., Stults, C. B., … & Halkitis, P. N. (2021). Ensuring survey research data integrity in the era of internet bots. *Quality &Amp; Quantity, 56*(4), 2841–2852. https://doi.org/10.1007/s11135-021-01252-1

Grigoras, M. & Wille, B. (2017). Shedding light on the dark side: associations between the dark triad and the dsm-5 maladaptive trait model. *Personality and Individual Differences, 104*, 516-521. https://doi.org/10.1016/j.paid.2016.09.016

HackerOne. (2021). The 2021 Hacker Report: Understanding hacker motivations, development and outlook. Retrieved from: https://www.hackerone.com/resources/reporting/the-2021-hacker-report?ungated=%3Futm_source&utm_medium=cpc&utm_campaign=2021_HR

HackerOne. (2025). HackerOne Community. Retrieved from: https://www.hackerone.com/platform/community#:~:text=The%20world's%20most%20elite%20security,ensuring%20your%20business%20stays%20secure

HackTheBox.com (2025). Player Database. Retrieved from: https://www.hackthebox.com/players#:~:text=Player%20Database,m%20individuals%20train%20with%20HTB

Hadi, M. A., Alldred, D. P., Closs, S. J., & Briggs, M. (2012). Mixed-methods research in pharmacy practice: basics and beyond (part 1). *International Journal of Pharmacy Practice, 21*(5), 341–345. https://doi.org/10.1111/ijpp.12010

Hare, R. D. (2003). *The Hare Psychopathy Checklist–Revised (2nd ed.)*. Toronto, Ontario, Canada: Multi-Health Systems.

Harms, P., Marbut, A., Johnston, A., Lester, P., & Fezzey, T. (2022). Exposing the darkness within: A review of dark personality traits, models and measures and their relationship to insider threats. *Journal of Information Security and Applications, 71*.

Haz, L., Rodríguez-García, M., & Fernández, A. (2022). Detecting narcissist dark triad psychological traits from Twitter. *Proceedings of the 14th International Conference on Agents and Artificial Intelligence*.

Hess, M. F. (2022). The Fyre fraud: A case exploring the dark triad personality. *Issues in Accounting Education*, *37*(3), 125-140. https://doi.org/10.2308/issues-2020-035

Hoang, T. T., Manso, P. H., Edman, S., Mercer-Rosa, L., Mitchell, L. E., Sewda, A., Dwartz, M., Fogel, M., Agopian, A., & Goldmuntz, E. (2019). Genetic variants of hif1α are associated with right ventricular fibrotic load in repaired tetralogy of Fallot patients: a cardiovascular magnetic resonance study. *Journal of Cardiovascular Magnetic Resonance, 21*(1), 51. https://doi.org/10.1186/s12968-019-0555-2

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2016). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology, 62*(6), 1720-1741. https://doi.org/10.1177/0306624x16679162

Holt, T. J., Lee, J. R., Liggett, R., Holt, K., & Bossler, A. M. (2019). Examining perceptions of online harassment among constables in England and Wales. *IJCIC, 2*(1), 24-39. https://doi.org/10.52306/02010319lfqz1592

Holt, T. J., Smirnova, O., & Chua, Y. (2016). The economic impact of stolen data markets., *Palgrave Studies in Cybercrime and Cybersecurity (PSCYBER).* 45-72. https://doi.org/10.1057/978-1-137-58904-0_3

Holt, T., Leukfeldt, R., & Weijer, S. (2020). An examination of motivation and routine activity theory to account for cyber-attacks against Dutch web sites. *Criminal Justice and Behavior, 47*(4), 487-505. https://doi.org/10.1177/0093854819900322

Hu, H., Liu, J., Jian-cheng, T., & Liu, J. (2020). Socmtd: selecting optimal countermeasure for moving target defense using dynamic game. *KSII Transactions on Internet and Information Systems, 14*(10). https://doi.org/10.3837/tiis.2020.10.013

Hudson, N. W. (2022). Lighten the darkness: personality interventions targeting Agreeableness also reduce participants' levels of the dark triad. *Journal of Personality, 91*(4), 901-916. https://doi.org/10.1111/jopy.12714

Hudson, N. W., & Fraley, R. C. (2015). Volitional personality trait change: Can people choose to change their personality traits? *Journal of Personality and Social Psychology*, *109*(3), 490–507. https://doi.org/10.1037/pspp0000021

Hudson, N. W., & Fraley, R. C. (2016). Do people's desires to change their personality traits vary with age? An examination of trait change goals across adulthood. *Social Psychological and Personality Science*, *7*, 847–856. https://doi.org/10.1177/1948550616657598

Hudson, N. W., Briley, D. A., Chopik, W. J., & Derringer, J. (2019). You have to follow through: Attaining behavioral change goals predicts volitional personality change. *Journal of Personality and Social Psychology*, *117*, 839–857. https://doi.org/10.1037/pspp0000221

Hussain, Z., Wegmann, E., & Griffiths, M. D. (2021). The association between problematic social networking site use, dark triad traits, and emotion dysregulation. *BMC Psychology*, *9*(1). https://doi.org/10.1186/s40359-021-00668-6

IBM Security, (2023). Cost of a Data Breach Report 2023.

IBM.com, (2024). What is zero trust? Retrieved from: https://www.ibm.com/topics/zero-trust?

Infosecinstitute.com, (2024). Penetration testing careers; what is a penetration tester? Retrieved from:https://resources.infosecinstitute.com/overview/penetration-testing-careers/#:~:text=According%20to%20the%20Bureau%20of,will%20be%20needed%20by%202031.

Ivankova, N., Creswell, J., & Stick, S. (2006). Using mixed-methods sequential explanatory design: from theory to practice. *Field methods, 18*(1), 3–20. https://doi.org/10.1177/1525822x05282260

Jajodia, S., Shakarian, P., Subrahmanian, V. S., Swarup, V., & Wang, C. (2015). Cyber Attribution: An Argumentation-Based Approach. In *Advances in Information Security* (Vol. 56, pp. 151–171). Springer International Publishing AG. https://doi.org/10.1007/978-3-319-14039-1_8

Ji, A., & Esqueda, A. P. (2022). The relationship between developmental factors and the big five personality traits. *JSR*, *11*(4).

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* (pp. 102–138). Guilford Press.

John, O. P., Donahue, E. M., & Kentle, R. L. (1991). The Big Five Inventory – Versions 4a and 54. *Institute of Personality and Social Research.*

John, O. P., Naumann, L. P., & Soto, C. J. (2008). Paradigm shift to integrative Big-Five Trait Taxonomy: History, Measurement and Conceptual Issues. *Handbook of personality: theory and research,* 114-158.

Johnson, C., et al., (2016). Guide to Cyber Threat Information Sharing. *NIST Special Publication 800-150*.

Johnson, L. K., Plouffe, R. A., & Saklofske, D. H. (2019). Subclinical sadism and the dark triad. *Journal of Individual Differences, 40*(3), 127-133. https://doi.org/10.1027/1614-0001/a000284

Joint Task Force, (2020). Security and Privacy Controls for Information Systems and Organizations. *NIST Special Publication 800-53*(5).

Jonason, P. K., Valentine, K. A., Li, N. P., & Harbeson, C. L. (2011). Mate-selection and the dark triad: facilitating a short-term mating strategy and creating a volatile environment. *Personality and Individual Differences, 51*(6), 759-763. https://doi.org/10.1016/j.paid.2011.06.025

Jonason, P. K., Żemojtel-Piotrowska, M., Piotrowski, J., Sedikides, C., Campbell, W. K., Gebauer, J. E., Maltby, J., Adamovic, M., Adams, B., Kadiyono, A. L., Atitsogbe, K., Bundhoo, H., Băltătescu, S., Billić, S., Brulin, J., Chobthamkit, P., Del Carmen, Dominguez, A., Dragova-Koleva, S., El-Astal, S., Esteves, C., Eldesoki, W., Gouveia, V., Gundolf, K., Illisko, D., Jauk, E., Kamble, S., Khachatryan, N., Klicperova-Baker, M., Knezovic, E., Kovacs, M., Lei, X., Liik, K., Mamuti, A., Rodrigo Moreta-Herrera, C., Milfront, T., Wei Ong, C., Osin, E., Park, J., Petrovic, B., Ramos-Diaz, J., Ridic, G., van den Bos, K., Van Hiel, A., Uslu, O., Wlodarczyk, A., & Yahiiaev, I. (2020). Country-level correlates of the dark triad traits in 49 countries. *Journal of Personality, 88*(6), 1252-1267. https://doi.org/10.1111/jopy.12569

Jonason, P. K., Kaźmierczak, I., Campos, A. C., & Davis, M. D. (2021). Leaving without a word: Ghosting and the dark triad traits. *Acta Psychologica*, *220*, 103425. https://doi.org/10.1016/j.actpsy.2021.103425

Jones, D. & Neria, A. (2015). The dark triad and dispositional aggression. *Personality and Individual Differences, 86*, 360-364. https://doi.org/10.1016/j.paid.2015.06.021

Jones, D. N. & Mueller, S. (2021). Is Machiavellianism dead or dormant? The perils of researching a secretive construct. *Journal of Business Ethics, 176*(3), 535-549. https://doi.org/10.1007/s10551-020-04708-w

Jones, D. N. & Paulhus, D. L. (2017). Duplicity among the dark triad: three faces of deceit. *Journal of Personality and Social Psychology, 113*(2), 329-342. https://doi.org/10.1037/pspp0000139

Jones, D. N., Padilla, E., Curtis, S. R., & Kiekintveld, C. (2021). Network discovery and scanning strategies and the dark triad. *Computers in Human Behavior, 122*, 106799. https://doi.org/10.1016/j.chb.2021.106799

Jones, D. N. (2022). Shadows behind the keyboard. *Proceedings of the 2022 ACM on International Workshop on Security and Privacy Analytics*.

Jones, D. N., & Paulhus, D. L. (2014). Introducing the short dark triad (SD3). *Assessment, 21,*(1), 28-41.

Kasneci, E., Sessler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., … & Kasneci, G. (2023). Chatgpt for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences, 103,* 102274. https://doi.org/10.1016/j.lindif.2023.102274

Kaufman, S. B., Yaden, D. B., Hyde, E., & Tsukayama, E. (2019). The light vs. dark triad of personality: contrasting two very different profiles of human nature. *Frontiers in Psychology, 10.* https://doi.org/10.3389/fpsyg.2019.00467

Kaufmann, L. M., Wheeler, M., & Sojo, V. (2021). Employment precarity strengthens the relationships between the dark triad and professional commitment. *Frontiers in Psychology, 12*. https://doi.org/10.3389/fpsyg.2021.673226

Kaya, A., Mukba, G., & Özok, H. İ. (2023). A person-centered approach to emotional security: Latent profile analysis of the dark triad and psychological symptoms. *Psychological Reports*. https://doi.org/10.1177/00332941231203561

Kennison, S. M., Jones, I. T., Spooner, V. H., & Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails. *Computers in Human Behavior Reports*, *4*, 100132. https://doi.org/10.1016/j.chbr.2021.100132

Kennison, S., & Chan-Tin, D., (2021). Predicting the Adoption of Password Managers* A Tale of Two Samples. Technology, *Mind & Society*.

Kernberg, O. (2016). What is personality? *Journal of Personality Disorders, 30*(2), 145-156.

Khando, K., Gao, S., Islam, M. S., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: a systematic literature review. *Computers &Amp; Security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

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

Kim, H., Kwon, H. J., & Kim, K. K. (2018). Modified cyber kill chain model for multimedia service environments. *Multimedia Tools and Applications, 78*(3), 3153–3170. https://doi.org/10.1007/s11042-018-5897-5

Kioskli, K. & Polemi, N. (2020). Measuring psychosocial and behavioural factors improves attack potential estimates. *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*. https://doi.org/10.23919/icitst51030.2020.9351343

Kioskli, K. & Polemi, N. (2020). Psychosocial approach to cyber threat intelligence. *International Journal of Chaotic Computing, 7*(1), 159-165. https://doi.org/10.20533/ijcc.2046.3359.2020.0021

Kircaburun, K., Jonason, P. K., & Griffiths, M. D. (2018). The Dark Triad traits and problematic social media use: The mediating role of cyberbullying and cyberstalking. *Personality and Individual Differences, 135*, 264–269. https://doi.org/10.1016/j.paid.2018.07.034

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social Engineering and the construction of the "Deficient user" in cybersecurity discourses. *Science, Technology, & Human Values*, *46*(6), 1316-1339. https://doi.org/10.1177/0162243921992844

Krick, A., Tresp, S., Vatter, M., Ludwig, A., & Wihlenda, M. (2016). The relationships between the dark triad, the moral judgment level, and the students' disciplinary choice. *Journal of Individual Differences, 37*(1), 24-30. https://doi.org/10.1027/1614-0001/a000184

Kumawat, V., Pal, P., & Jha, P. K. (2023). Ethical hacking: white hat hackers. *SCRS Proceedings of International Conference of Undergraduate Students,* 13-17. https://doi.org/10.52458/978-81-95502-01-1-2

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications, 34*(18), 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

Laakasuo, M., Repo, M., Berg, A., Drosinou, M., Kunnari, A., Koverola, M., Saikkonen, T., Hannikainen, I. R., Visala, A., & Sundvall, J. R. (2020). The dark path to eternal life: Machiavellianism predicts approval of mind upload technology. *Personality and Individual Differences*, *177*. https://doi.org/10.31234/osf.io/smqu4

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*(1), 159–174. https://doi.org/10.2307/2529310

Lazarov, A. and Petrova, P. (2022). Modelling activity of a malicious user in computer networks. *Cybernetics and Information Technologies, 22*(2), 86-95. https://doi.org/10.2478/cait-2022-0018

Lee, K., Ashton, M. C., Wiltshire, J., Bourdage, J. S., Visser, B. A., & Gallucci, A. (2013). Sex, power, and money: prediction from the dark triad and honesty–humility. *European Journal of Personality, 27*(2), 169-184. https://doi.org/10.1002/per.1860

Lee, S. (2019). Predicting sns addiction with the big five and the dark triad. *Cyberpsychology Journal of Psychosocial Research on Cyberspace, 13*(1). https://doi.org/10.5817/cp2019-1-3

Liang, W., Tadesse, G. A., Ho, D. E., Li, F., Zaharia, M., Zhang, C., … & Zou, J. (2022). Advances, challenges, and opportunities in creating data for trustworthy AI. *Nature Machine Intelligence, 4*(8), 669-677. https://doi.org/10.1038/s42256-022-00516-1

Lim, S. & Shim, H. (2022). No secrets between the two of us: privacy concerns over using ai agents. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16*(4). https://doi.org/10.5817/cp2022-4-3

Lingnau, V., Fuchs, F., & Beham, F. (2022). The link between corporate sustainability and willingness to invest: new evidence from the field of ethical investments. *Journal of Management Control, 33*(3), 335-369. https://doi.org/10.1007/s00187-022-00340-z

Liu, F. W. (2024). Exploring vulnerabilities and protections in large language models: a survey. *arxiv*. https://arxiv.org/html/2406.00240v1#bib.bib16

Liu, F., Gao, H., & Wei, Z. (2020). Research on the game of network security attack-defense confrontation through the optimal defense strategy. *Security and Privacy, 4*(1). https://doi.org/10.1002/spy2.136

Luo, J., Zhang, B., Cao, M., & Roberts, B. W. (2023). The stressful personality: A meta-analytical review of the relation between personality and stress. *Personality and Social Psychology Review*, *27*(2), 128-194.

Lyons, M., & Jonason, P. K. (2015). Dark triad, tramps, and thieves. *Journal of Individual Differences*.

Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports, 7*, 7999-8012.

Ma, X., Yi, Y., Luo, Y., Wajahat, A., & Nazir, A. (2023). Hacker community detection in online social network: a case study. *Third International Conference on Green Communication, Network, and Internet of Things (CNIoT 2023).* https://doi.org/10.1117/12.3010341

Maasberg, M., Slyke, C. V., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM, 63*(12), 64-80. https://doi.org/10.1145/3408864

Maasberg, M., Warren, J., & Beebe, N., (2015). The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits. *IEEE 2015 48th Hawaii International Conference on System Science*. DOI 10.1109/HICSS.2015.423

Maftei, A., Holman, A., & Elenescu, A. (2022). The Dark Web of machiavellianism and psychopathy: Moral disengagement in IT organizations. *Europe's Journal of Psychology*, *18*(2), 181-192. https://doi.org/10.5964/ejop.4011

Maimon, D., et al., (2017). Re-Thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors fore Predicting Cyber-attacks. *EBCS Procedings.*

Mammadov, S. (2022). Big Five personality traits and academic performance: A meta-analysis. *Journal of Personality*, *90*(2), 222–255. https://doi.org/10.1111/jopy.12663

Marengo, D., Sindermann, C., Häckel, D., Settanni, M., Elhai, J. D., & Montag, C. (2020). The association between the Big Five personality traits and smartphone use disorder: A meta-analysis. *Journal of Behavioral Addictions*, *9*(3), 534-550.

Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., and Clark., J. (2024). The AI Index 2024 Annual Report. AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA. Retrieved from: https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf.

Matheus, T. and Sarma, M. (2015). Knowledge creation in virtual communities – exploring practices in open source software hacker communities. *The International Technology Management Review, 5*(2), 94. https://doi.org/10.2991/itmr.2015.5.2.4

Matulessy, A., & Humaira, N., (2016). Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits. *Psychology and Behavioral Sciences, 5*(6).

Maxmillian, J. M., & Sinha, G. (2022). How Organizations Become Exposed to Certain Cyber-attacks or Breaches and Ways to Mitigate. *NeuroQuantology*, *20*(6), 4271-4279.

McBride, M., Carter, L., & Phillips, B. (2018). Exploring cybersecurity workforce personality traits. *Computers & Security, 73*, 345–356. https://doi.org/10.1016/j.cose.2017.11.007

McCambridge, J., Kalaitzaki, E., White, I. R., Khadjesari, Z., Murray, E., Linke, S., … & Wallace, P. (2011). Impact of length or relevance of questionnaires on attrition in online trials: randomized controlled trial. *Journal of Medical Internet Research, 13*(4), e96. https://doi.org/10.2196/jmir.1733

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

McCrae, R. (1991). The Five-Factor Model and its assessment in clinical settings. *Journal of Personality Assessment, 57(3),* 399-414. https://doi.org/10.1207/s15327752jpa5703_2

McCrae, R. R., & Costa, P. T. Jr. (1997). Personality trait structure as a human universal. *American Psychologist, 52*(5), 509–516. https://doi.org/10.1037/0003-066X.52.5.509

Measelle, J. R., John, O. P., Ablow, J. C., Cowan, P. A., & Cowan, C. P. (2005). Can children provide coherent, stable, and valid self-reports of the Big Five dimensions? A longitudinal study from ages 5 to 7. *Journal of Personality and Social Psychology, 89*(1), 90-106. https://doi.org/10.1037/0022-3514.89.1.90

Miao, Y., Wang, J., Shen, R., & Wang, D. (2023). Effects of big five, hexaco, and dark triad on counterproductive work behaviors: a meta-analysis. *International Journal of Mental Health Promotion, 25*(3), 357-374. https://doi.org/10.32604/ijmhp.2023.027950

Miller, T. J., Baranski, E. N., Dunlop, W. L., & Ozer, D. J. (2019). Striving for change: The prevalence and correlates of personality change goals. *Journal of Research in Personality*, *80*, 10–16. https://doi.org/10.1016/j.jrp.2019.03.010

Mills, H., Crone, D., James, D., & Johnston, L. (2012). Exploring the perceptions of success in an exercise referral scheme. *Evaluation Review, 36*(6), 407–429. https://doi.org/10.1177/0193841x12474452

Mischel, W., & Shoda, Y. (1995). A cognitive-affective system theory of personality: Reconceptualizing situations, dispositions, dynamics, and invariance in personality structure. *Psychological Review*, *102*(2), 246–268.

MITRE ATT&CK. (2026). MITRE ATT&CK Matrix. Retrieved from: https://attack.mitre.org/

Mohammad, N. A. N., Yassin, W., Ahmad, R., Hassan, A., & Al-Mhiqani, M. N. (2019). An insider threat categorization framework for an automated manufacturing execution system. *International Journal of Innovation in Enterprise System, 3*(02), 31–41. https://doi.org/10.25124/ijies.v3i02.38

Muris, P., Merckelbach, H., Otgaar, H., & Meijer, E. H. (2017). The malevolent side of human nature. *Perspectives on Psychological Science, 12*(2), 183-204. https://doi.org/10.1177/1745691616666070

Musek, J. and Grum, D. K. (2021). The bright side of personality. *Heliyon*, *7*(3), e06370. https://doi.org/10.1016/j.heliyon.2021.e06370

Naz, M., Subhan, S., & Saleem, S. (2022). Emotion regulation, dark triad personality, rule-breaking behavior and mental health problems in young adults: structural equation modelling. *Journal of Professional &Amp; Applied Psychology, 3*(4), 437-452. https://doi.org/10.52053/jpap.v3i4.126

Neuert, C. and Lenzner, T. (2019). Effects of the number of open-ended probing questions on response quality in cognitive online pretests. *Social Science Computer Review, 39*(3), 456-468. https://doi.org/10.1177/0894439319866397

Neufeld, D. J. (2023). Computer crime motives: Do we have it right? *Sociology Compass, 17*(4). https://doi.org/10.1111/soc4.13077

Neumann, C., Jones, D. N., & Paulhus, D. (2021). Modeling dark personalities. *Dark Triad and Corporate Climate Lab.*

Nicholls, A., Madigan, D., Duncan, L., Hallward, L., Lazuras, L., Bingham, K., … & Fairs, L. (2019). Cheater, cheater, pumpkin eater: the dark triad, attitudes towards doping, and cheating behaviour among athletes. *European Journal of Sport Science, 20*(8), 1124-1130. https://doi.org/10.1080/17461391.2019.1694079

Nieles, M., et al. (2017). An Introduction to Information Security. *NIST Special Publication 800-12* (1). https://doi.org/10.6028/NIST.SP.800-12r1

Nocera, T. and Dahlen, E. (2020). Dark triad personality traits in cyber aggression among college students. *Violence and Victims, 35*(4), 524-538. https://doi.org/10.1891/vv-d-18-00058

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

O'Boyle, E.H., Forsyth, D.R., Banks, G.C., Story, P.A., White, C.D., (2015). A meta-analytic test of redundancy and relative importance of the dark triad and Five-Factor model of personality. *Journal of Personality, 83,* 644-664.

O'Brien, K. K., Solomon, P., Worthington, C., Ibáñez-Carrasco, F., Baxter, L., Nixon, S., … & Zack, E. (2014). Considerations for conducting web-based survey research with people living with human immunodeficiency virus using a community-based participatory approach. *Journal of Medical Internet Research, 16*(3), e81. https://doi.org/10.2196/jmir.3064

Ock, J. (2023). How dark is the core of dark personality traits? Examining the effect of temporal separation between measures on the commonality among the dark triad personality traits. https://doi.org/10.2139/ssrn.4446731

Ock, J., Heo, G. Y., & Kweon, M. (2023). HEXACO personality traits and self-control as predictors of counterproductive academic behavior. *PsyArXiv Preprints.* https://doi.org/10.31234/osf.io/2g7fn

Office of Public Affairs. (2020, February 21). *Wells Fargo agrees to pay $3 billion to resolve criminal and civil investigations into sales practices involving the opening of millions of accounts without customer authorization. Department of Justice | United States Department of Justice*. https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices

Okpa, J. T., Ugwuoke, C. U., Ajah, B. O., Eshiotse, E., Igbe, J. E., Ajor, O. J., Okoi, O. N., Eteng, M. J., & Nnamani, R. G. (2022). Cyberspace, Black-hat hacking and economic sustainability of corporate organizations in cross-river state, Nigeria. *SAGE Open*, *12*(3), 215824402211227. https://doi.org/10.1177/21582440221122739

Olufunsho, F., et al. (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE, 10,* 134038. doi: 10.1109/ACCESS.2022.3231847

O'Neill, M., & Connor, M. (2023). Amplifying limitations, harms, and risks of Large Language Models. *arXiv*. https://arxiv.org/abs/2307.04821

Paas, F., Gog, T. v., & Sweller, J. (2010). Cognitive load theory: new conceptualizations, specifications, and integrated research perspectives. *Educational Psychology Review, 22*(2), 115-121. https://doi.org/10.1007/s10648-010-9133-8

Padayachee, K. (2022). Understanding the effects of situational crime prevention and personality factors on insider compliance. *Journal of Information Security and Applications*, *70*, 103338. https://doi.org/10.1016/j.jisa.2022.103338

Pan, A., Jun Shern Chan, Zou, A., L., N., Basart, S., Woodside, T., Ng, J., Zhang, H., Emmons, S., & Hendrycks, D. (2023). Do the Rewards Justify the Means? Measuring Trade-Offs Between Rewards and Ethical Behavior in the MACHIAVELLI Benchmark. *arXiv*. https://doi.org/10.48550/arxiv.2304.03279

Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., Pallis, E., & Markakis, E. K. (2021). A survey on human and personality vulnerability assessment in cybersecurity: Challenges, approaches, and open issues. *arXiv*.

Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018). Characterizing eve: analysing cybercrime actors in a large underground forum. *Research in Attacks, Intrusions, and Defenses,* 207–227. https://doi.org/10.1007/978-3-030-00470-5_10.

Paulhus, D. L. (1991). Measurement and control of response bias. In J. P. Robinson, P. R. Shaver, & L. S. Wrightsman (Eds.), *Measures of personality and social psychological attitudes* (pp. 17–59). Academic Press.

Paulhus, D. L., Buckels, E. E., Trapnell, P. D., & Jones, D. N. (2021). Screening for dark personalities. *European Journal of Psychological Assessment, 37*(3), 208-222. https://doi.org/10.1027/1015-5759/a000602

Paulhus, D.L. (2014). Toward a taxonomy of dark personalities. *Current Directions in Psychological Science, 23,* 421-426.

Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, *36*(6), 556-563. https://doi.org/10.1016/s0092-6566(02)00505-6

Perez, E., Huang, S., Song, F., Cai, T., Ring, R., Aslanides, J., Glaese, A., McAleese, N., & Irving, G. (2022). Red teaming language models with language models. *Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing*. https://doi.org/10.18653/v1/2022.emnlp-main.225

Perkins, R. C. (2022). The illicit ecosystem of hacking: a longitudinal network analysis of website defacement groups. *Social Science Computer Review*. https://doi.org/10.1177/08944393221097881

Petry, R. A. (2011). Imperfect duties and corporate philanthropy: A Kantian approach. *Journal of Business Ethics*, *106*(3), 367-381. https://doi.org/10.1007/s10551-011-1002-y

Povše, D. F. (2019). Protecting human rights through a global encryption provision. *Security and Law*, 129-160. https://doi.org/10.1017/9781780688909.006

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

Pratama, A. R., Firmansyah, F. M., & Rahma, F. (2022). Security awareness of single sign-on accounts in the academic community: the roles of demographics, privacy concerns, and Big-Five personality: *PeerJ Computer Science*, *8*, e918.

Quintus, M., Egloff, B., & Wrzus, C. (2017). Predictors of volitional personality change in younger and older adults: Response surface analyses signify the complementary perspectives of the self and knowledgeable others. *Journal of Research in Personality*, *70*, 214–228. https://doi.org/10.1016/j.jrp.2017.08.001

Raja, A., Spertus, J. A., Yeh, R. W., & Secemsky, E. A. (2020). Assessing health-related quality of life among patients with peripheral artery disease: a review of the literature and focus on patient-reported outcome measures. *Vascular Medicine, 26*(3), 317-325. https://doi.org/10.1177/1358863x20977016

Rantanen, J., Metsäpelto, R., Feldt, T., Pulkkinen, L., & Kokko, K. (2007). Long-term stability in the big five personality traits in adulthood. *Scandinavian Journal of Psychology, 48*(6), 511-518. https://doi.org/10.1111/j.1467-9450.2007.00609.x

Rauthmann, J. F. (2011). The dark triad and interpersonal perception: similarities and differences in the social consequences of narcissism, Machiavellianism, and psychopathy. *Social Psychological and Personality Science, 3*(4), 487-496. https://doi.org/10.1177/1948550611427608

Raywood-Burke, G., Bishop, L., Asquith, P. M., & Morgan, P. L. (2021). Human individual difference predictors in cyber-security: exploring an alternative scale method and data resolution to modelling cyber secure behavior. *HCI for Cybersecurity, Privacy, and Trust,* 226–240. https://doi.org/10.1007/978-3-030-77392-2_15

Rege, A. (2013). Factors impacting attacker decision-making in power grid cyber-attacks. *Critical Infrastructure Protection VII*, 125–138. https://doi.org/10.1007/978-3-642-45330-4_9

Roberts, B. W., & Yoon, H. J. (2022). Personality psychology. *Annual Review of Psychology*, *73*(5), 489–516. https://doi.org/10.1146/annurev-psych-020821-114927

Roer-Strier, D. and Kurman, J. (2009). Combining qualitative and quantitative methods to study perceptions of immigrant youth. *Journal of Cross-Cultural Psychology, 40*(6), 988-995. https://doi.org/10.1177/0022022109349480

Rogoza, R., & Cieciuch, J. (2019). Dark triad traits and their structure: An empirical approach. *Current Psychology*, *39*(4), 1287-1302. https://doi.org/10.1007/s12144-018-9834-6

Romagna, M. (2019). Hacktivism: Conceptualization, techniques, and historical view. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 1-27. https://doi.org/10.1007/978-3-319-90307-1_34-1

Romanosky, S., & Boudreaux, B. (2021). Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. *International Journal of Intelligence and Counterintelligence*, *34*(3), 463–493. https://doi.org/10.1080/08850607.2020.1783877

Rosenbaum, M. H. (2010). Giannis stamatellos: computer ethics—a global perspective. *Ethics and Information Technology, 12*(4), 371-373. https://doi.org/10.1007/s10676-010-9246-2

Russell, J. D., Weems, C. F., Ahmed, I., & Richard, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security Technology, 1*(3-4), 163-174. https://doi.org/10.1080/23742917.2017.1345271

Sailio, M., et al. (2020). Cyber Threat Actors for the Factory of the Future. *Applied Sciences, 10*, 4334.

Saldaña, J. (2015). Thinking qualitatively: methods of mind. *SAGE Publications, Inc., 1.* https://doi.org/10.4135/9781071909782

Saldaña, J. (2021). The coding manual for qualitative researchers. *The coding manual for qualitative researchers*, 1-440.

Saleh, A. and Bista, K. (2017). Examining factors impacting online survey response rates in educational research: perceptions of graduate students. *Journal of MultiDisciplinary Evaluation, 13*(29), 63-74. https://doi.org/10.56645/jmde.v13i29.487

Sammut, R., Griscti, O., & Norman, I. (2021). Strategies to improve response rates to web surveys: a literature review. *International Journal of Nursing Studies, 123*, 104058. https://doi.org/10.1016/j.ijnurstu.2021.104058

Sanders, H. (2021). Dark traits and hacking potential. *Journal of Organizational Psychology*, *21*(3). https://doi.org/10.33423/jop.v21i3.4307

Schyns, B., Wisse, B., & Sanders, S. (2019). Shady strategic behavior: recognizing strategic followership of dark triad followers. *Academy of Management Perspectives, 33*(2), 234-249. https://doi.org/10.5465/amp.2017.0005

Scott, P. & Briggs, J. (2009). A pragmatist argument for mixed methodology in medical informatics. *Journal of Mixed Methods Research, 3*(3), 223–241. https://doi.org/10.1177/1558689809334209

Sebastian, G. (2023). Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information. *SSRN Electronic Journal*.

Selzer, N., & Oelrich, S. (2021). Saint or Satan? Moral development and dark triad influences on Cybercriminal intent. *Cybercrime in Context*, 175-194. https://doi.org/10.1007/978-3-030-60527-8_11

Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., & Kambhampati, S. (2020). A survey of moving target defenses for network security. *IEEE Communications Surveys &Amp; Tutorials, 22*(3), 1909-1941. https://doi.org/10.1109/comst.2020.2982955

Shackelford, S., Boustead, A., & Makridis, C. (2021). Defining "reasonable" cybersecurity: lessons from the states. *Available at SSRN 3919275*.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media*, *9*(4), 475–480.

Shires, J. (2019). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, *41*(1), 82-107. https://doi.org/10.1080/13523260.2019.1670006

Silic, M., & Lowry, P. B. (2019). Breaking bad in cyberspace: Understanding why and how Black Hat hackers manage their nerves to commit their virtual crimes. *Information Systems Frontiers*, *23*(2), 329-341. https://doi.org/10.1007/s10796-019-09949-3

Soutter, A. R. B., Bates, T. C., & Mõttus, R. (2020). Big Five and HEXACO personality traits, proenvironmental attitudes, and behaviors: A meta-analysis. *Perspectives on Psychological Science*, *15*(4), 913-941.

Spector, A. & Pinto, R. (2015). Partnership matters in health services research: a mixed methods study of practitioners' involvement in research and subsequent use of evidence-based interventions. *Journal of Mixed Methods Research, 11*(3), 374-393. https://doi.org/10.1177/1558689815619823

Statista (2025). Cybersecurity skill gaps – statistics and facts. Retrieved from: https://www.statista.com/topics/11872/cybersecurity-skills-gaps/#topicOverview

Stoltenberg, S. F., Batien, B. D., & Birgenheir, D. G. (2008). Does gender moderate associations among impulsivity and health-risk behaviors? *Addictive Behaviors, 33*(2), 252–265. https://doi.org/10.1016/j.addbeh.2007.09.004

Storozuk, A., Ashley, M., Delage, V., & Maloney, E. A. (2020). Got bots? Practical recommendations to protect online survey data from bot attacks. *The Quantitative Methods for Psychology, 16*(5), 472–481. https://doi.org/10.20982/tqmp.16.5.p472

Straub, J. (2020). Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks. *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, 148–153.

Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. (2018). MITRE ATT&CK®: Design and Philosophy; The MITRE Corporation: Bedford, MA, USA, 2018.

Sweller, J. (2010). Element interactivity and intrinsic, extraneous, and germane cognitive load. *Educational Psychology Review, 22*(2), 123–138. https://doi.org/10.1007/s10648-010-9128-5

Tabachnick, B. G., & Fiddell, L. S. (2019). *Using multivariate statistics* (7th edition).

Tamrakar, A., Russell, J. D., Ahmed, I., Richard, G. G., & Weems, C. F. (2016). Spice. *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy.* https://doi.org/10.1145/2857705.2857744

Tanczer, L. M. (2019). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. *Contemporary Security Policy*, *41*(1), 108-128. https://doi.org/10.1080/13523260.2019.1669336

Tang, B., Wang, J., Qiu, H., Yu, J., Yu, Z., & Liu, S. (2023). Attack behavior extraction based on heterogeneous cyberthreat intelligence and graph convolutional networks. *Computers, Materials &Amp; Continua, 74*(1), 235-252. https://doi.org/10.32604/cmc.2023.029135

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for apt-style attacks. *Heliyon, 7*(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2,* 53–55.

Thomas, G., Burmeister, O., & Low, G. (2018). Issues of implied trust in ethical hacking. *The ORBIT Journal, 2*(1), 1-19. https://doi.org/10.29297/orbit.v2i1.77

Thomas, G., Burmeister, O., & Low, G. (2019). The importance of ethical conduct by penetration testers in the age of breach disclosure laws. *Australasian Journal of Information Systems, 23*. https://doi.org/10.3127/ajis.v23i0.1867

Troisi, O., Maione, G., Grimaldi, M., & Loia, F. (2020). Growth hacking: Insights on data-driven decision-making from three firms. *Industrial Marketing Management*, *90*, 538-557.

TryHackMe. (2025). Four million users on TryHackMe! Retrieved from: https://tryhackme.com/resources/blog/four-million-on-tryhackme

U.S. Department of Homeland Security (2024). Homeland threat assessment 2024. Retrieved from: https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

Uebelacker, S. & Quiel, S. (2014). The Social Engineering personality framework. *4th Workshop on Socio-Technical Aspects in Security and Trust.* DOI 10.1109/STAST.2014.12

Usman, A., Hudain, M. A., Zainuddin, M. S., Jariono, G., & Fauzan, M. M. (2021). Educational strategies and roles of stakeholders in reducing antisocial behavior of football supporters. *Journal Cakrawala Pendidikan, 40*(3), 799-807. https://doi.org/10.21831/cp.v40i3.43947

Van de Weijer, S., & Leukfeldt, E., 2017. Big Five Personality Traits and Cybercrime Victims. *Cyberpsychology, Behavior and Social Networking, 00*.

Van der Schyff, K., Flowerday, S., & Lowry, P. B. (2020). Information privacy behavior in the use of Facebook apps: A personality-based vulnerability assessment. *Heliyon*, *6*(8). https://doi.org/10.1016/j.heliyon.2020.e04714

Vávra, J., Komárek, A., Grün, B., & Malsiner-Walli, G. (2022). Clusterwise multivariate regression of mixed-type panel data. *Preprint.* https://doi.org/10.21203/rs.3.rs-1882841/v1

Vedel, A. & Thomsen, D. (2017). The dark triad across academic majors. *Personality and Individual Differences, 116,* 86-91. https://doi.org/10.1016/j.paid.2017.04.030

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157-178.

Verizon (2023). DBIR 2023 Data Breach Investigations Report. 2023. *DBIR*.

Verizon, (2022). DBIR 2022 Data Breach Investigations Report. 2022. *DBIR*.

Verizon, (2024). DBIR 2024 Data Breach Investigations Report. *2024. DBIR*.

Verma, J., & Abdel-Salam, A. (2019). Testing Statistical Assumptions in Research. *John Wiley & Sons*. https://doi.org/10.1002/9781119528388

Veselka, L., Schermer, J. A., & Vernon, P. A. (2011). Beyond the big five: the dark triad and the supernumerary personality inventory. *Twin Research and Human Genetics, 14*(2), 158-168. https://doi.org/10.1375/twin.14.2.158

Votipka, D., Zhang, E., & Mazurek, M. L. (2021). HackEd: A pedagogical analysis of online vulnerability discovery exercises. *2021 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp40001.2021.00092

Wagner, J., Bolgan, S., & Rusconi, E. (2022). On the relation between hacking and autism or autistic traits: A systematic review of the scientific evidence. *Cybersecurity and Cognitive Science*, 157-196.

Wang, B. & Liu, B. (2023). A network deception defense mechanism based on virtual topology generation. *International Conference on Intelligence Systems, Communications, and Computer Networks (ISCCN 2023), 12702.* https://doi.org/10.1117/12.2679362

Wang, C., Freire, S. Zhang, M., Wei, J., Goncalves, J., Kostakos, V., Sarsenbayeva, Z., Schneegass, C., Bozzon, A., & Niforatos, E. (2023). Safeguarding Crowdsourcing Surveys from ChatGPT with Prompt Injection. *arXiv*. https://doi.org/10.48550/arxiv.2306.08833

Wang, Q. H., Zhang, L., & Qiao, M. (2017). Online hacker forum censorship: would banning the bad guys attract good guys? *Proceedings of the 50th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2017.677

Wang, X., Zhang, S., & Tao, X. (2022). Item response theory analysis of the dark factor of personality scale for college students in China. *International Journal of Environmental Research and Public Health, 19*(19), 12787. https://doi.org/10.3390/ijerph191912787

Warikoo, A. (2021). The Triangle Model for Cyber Threat Attribution. *Journal of Cyber Security*, *5*(3–4), 191–208. https://doi.org/10.1080/23742917.2021.1895532

Woods, D., & Allspaw, J. (2020). Revealing the Critical Role of Human Performance in Software. *Communications of the ACM, 63*(5).

Wu, M., Zhao, K., & Fils-Aime, F. (2022). Response rates of online surveys in published research: a meta-analysis. *Computers in Human Behavior Reports, 7*, 100206. https://doi.org/10.1016/j.chbr.2022.100206

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4), 64-74. https://doi.org/10.1145/2436256.2436272

Yan, L., Sha, L., Zhao, L., Li, Y., Martinez-Maldonado, R., Chen, G., … & Gašević, D. (2023). Practical and ethical challenges of large language models in education: a systematic scoping review. *British Journal of Educational Technology, 55*(1), 90-112. https://doi.org/10.1111/bjet.13370

Yeboah-Ofori, A. & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future Internet, 11*(3), 63. https://doi.org/10.3390/fi11030063

Yilmaz, Y, & Cetin, O., (2023). Personality Types and Ransomware Victimization. *Digital Threats: Research and Practice, 4*(4).

Yin, K., Li, D., Zhang, X., Dong, N., & Sheldon, O. J. (2023). The influence of the Big Five and Dark Triad personality constructs on knowledge sharing: A meta-analysis. *Personality and Individual Differences*, *214*. https://doi.org/10.2139/ssrn.4384432

Yong-ping, Z., Wang, J., Chen, Y., & Xia, L. (2018). Consideration of future consequences (cfc) serves as a buffer against aggression related to psychopathy. *Plos One, 13*(9), e0203663. https://doi.org/10.1371/journal.pone.0203663

Yoon Lee, S., Yao, M. Z., & Yi-Fan Su, L. (2021). Expressing unpopular opinion or trolling: Can dark personalities differentiate them? *Telematics and Informatics*, *63*, 101645. https://doi.org/10.1016/j.tele.2021.101645

Zell, E., & Lesick, T. L. (2022). Big five personality traits and performance: A quantitative synthesis of 50+ meta-analyses. *Journal of personality*, *90*(4), 559-573.

Zhang, H. & Zhao, H. (2020). Dark personality traits and cyber aggression in adolescents: a moderated mediation analysis of belief in virtuous humanity and self-control. *Children and Youth Services Review, 119*, 105565. https://doi.org/10.1016/j.childyouth.2020.105565

Zhang, Z., Bian, S., Zhao, H., & Qi, C. (2022). Dark triad and cyber aggression among Chinese adolescents during COVID-19: a moderated mediation model. *Frontiers in Psychology, 13*. https://doi.org/10.3389/fpsyg.2022.1011123

APPENDIX A. MITRE ATT&CK MATRIX

MITRE ATT&CK Matrix, which can be viewed at

https://attack.mitre.org/versions/v16/matrices/enterprise/

List of MITRE ATT&CK Tactics and Techniques

Reconnaissance
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites

Resource Development
Acquire Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities

Initial Access
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise

Trusted Relationship
Valid Accounts

Execution

Cloud Administration Command
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation

Persistence

Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Host Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Power Settings
Pre-OS Boot
Scheduled Task/Job
Server Software Component

Traffic Signaling
Valid Accounts

Privilege Escalation

Abuse Elevation Control Mechanism
Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain or Tenant Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts

Defense Evasion

Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Impersonation

Indicator Removal
Indirect Command Execution
Masquerading
Modify Authentication Process
Modify Cloud Compute Infrastructure
Modify Cloud Resource Hierarchy
Modify Registry
Modify System Image
Network Boundary Bridging
Obfuscated Files or Information
Plist File Modification
Pre-OS Boot
Process Injection
Reflective Code Loading
Rogue Domain Controller
Rootkit
Subvert Trust Controls
System Binary Proxy Execution
System Script Proxy Execution
Template Injection
Traffic Signaling
Trusted Developer Utilities Proxy Execution
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material
Valid Accounts
Virtualization/Sandbox Evasion
Weaken Encryption
XSL Script Processing

Credential Access

Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing

OS Credential Dumping
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Unsecured Credentials

Discovery

Account Discovery
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
System Information Discovery
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion

Lateral Movement

Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material

Collection

Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Video Capture

Command and Control

Application Layer Protocol
Communication Through Removable Media
Content Injection
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels

Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web Service

Exfiltration

Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account

Impact

Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot

APPENDIX B. CODEBOOK

Coding Categories

Table B1.

Dark Triad–Related Behaviors

Code	Definition	Keywords	Hypothesis	Example
BOLD	Direct, aggressive, or obvious attack approaches that show little concern for detection.	bold, aggressive, direct attack, brute force, obvious, frontal	Individuals high on Dark Triad traits will favor bold techniques.	"Launch a direct brute-force attack on the login portal."
DECEPTIVE	Use of false identities, impersonation, or misleading tactics.	fake, disguise, impersonate, deceive, spoof, masquerade	Individuals high on Dark Triad traits will favor deceptive techniques.	"Create fake employee credentials to gain access."
HIGH RISK	Tactics with high probability of detection or exposure.	risky, loud, obvious, detectable, dangerous	Individuals high on Dark Triad traits will favor high-risk techniques.	"Perform loud network scans likely to trigger alerts."

Table B2.

Big Five–Related Behaviors

Code	Definition	Keywords	Hypothesis	Example
CREATIVE	Novel or unconventional approaches to intrusion.	creative, innovative, novel, unique, unconventional	Individuals high in Openness will favor creative techniques.	"Use an unusual attack vector through IoT devices."
SOPHISTICATED	Complex, technically elaborate, multi-stage attacks.	sophisticated, advanced, complex, multi-stage	Individuals high in Openness and Conscientiousness will favor sophisticated techniques.	"Deploy a multi-stage APT campaign with custom malware."
STRUCTURED	Systematic, organized, or planned methods.	systematic, methodical, organized, structured, planned	Individuals high in Conscientiousness will prefer structured approaches.	"Follow a systematic reconnaissance methodology."
LOW RISK	Cautious and stealthy tactics designed to minimize detection.	cautious, stealthy, undetectable, careful	Individuals high in Conscientiousness will prefer low-risk approaches.	"Use passive reconnaissance to avoid detection."
SOCIAL ENGINEERING	Psychological manipulation or deception of human targets.	phishing, email, phone, impersonate, human	Individuals high in Extraversion will use Social Engineering tactics.	"Call employees pretending to be IT support."
AGGRESSIVE	Forceful or destructive actions aimed at damage or control.	aggressive, destructive, attack, destroy	Individuals low in Agreeableness will use aggressive methods.	"Deploy destructive malware to damage systems."

Table B3.

Specific Tactical Behaviors

Code	Definition	Keywords	Research Question	Example
PERSISTENT	Repeated attempts despite detection or failure.	persist, continue, retry, multiple attempts	Do participants high in Dark Triad traits show greater persistence?	"Continue attacking even after detection."
EVASIVE	Actions taken to hide identity or avoid detection.	evade, hide, cover tracks, anonymous	How do high Dark Triad scorers differ in evasion tactics?	"Use VPNs and proxies to hide identity."
RANSOMWARE	Deployment of encryption-based extortion attacks.	ransom, encrypt, payment, bitcoin	Are certain Dark Triad traits predictive of ransomware use?	"Encrypt files and demand payment."
PRIVILEGE ESCALATION	Attempts to gain higher-level system access.	escalate, admin, root, elevated	Are certain traits predictive of privilege escalation?	"Exploit vulnerabilities to gain admin rights."
LATERAL MOVEMENT	Expansion of access across network systems.	lateral, move, pivot, spread	Are certain traits predictive of lateral movement?	"Use compromised credentials to access other systems."
RECONNAISSANCE	Information gathering and target profiling.	scan, probe, enumerate, discover	Are some traits more predictive in reconnaissance stages?	"Scan network for vulnerable services."

Coding Procedure

Data Preparation

- Combined all open-ended responses for each participant.
- Standardized and cleaned text data (lowercasing, punctuation removal).

Keyword Matching

- Binary-coded based on the presence (*1*) or absence (*0*) of keywords.
- Applied inclusive OR logic (any keyword match = present).
- Manually reviewed ambiguous cases for accuracy.

Quality Assurance

- Checked for logical contradictions.
- Final codes validated through peer review and consensus checking.
- Verified interrater reliability (κ = .98; Landis & Koch, 1977).

APPENDIX C. SURVEY

Figure C1.

Recruitment Script

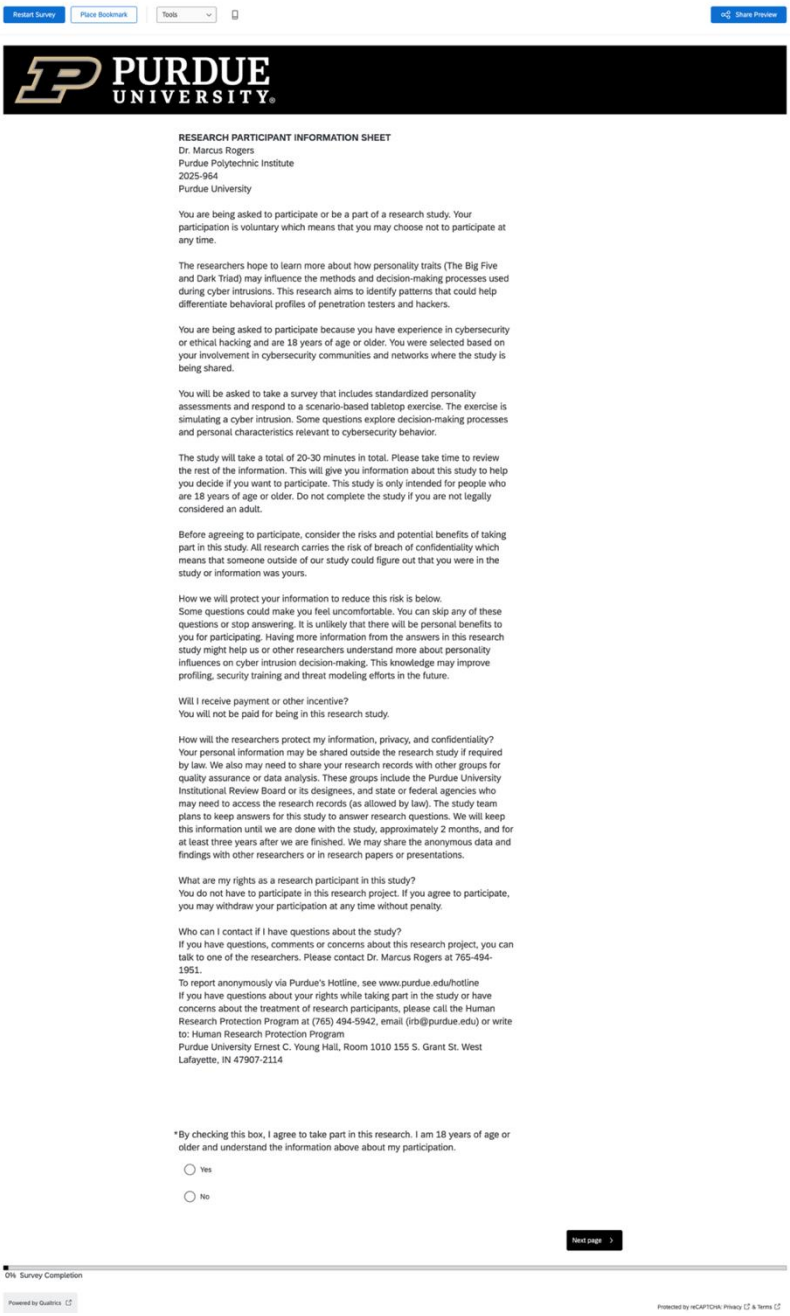


Figure C2.

Eligibility

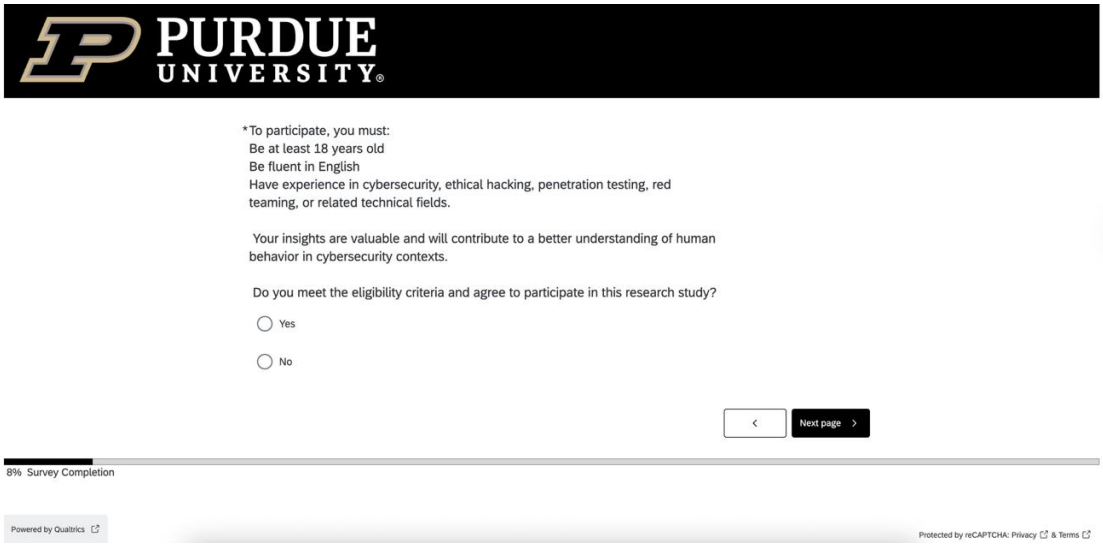


Figure C3.

Bot Prevention

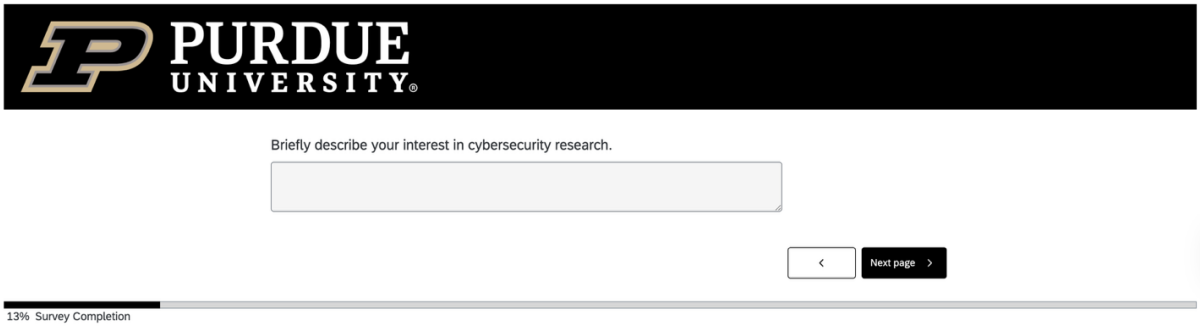
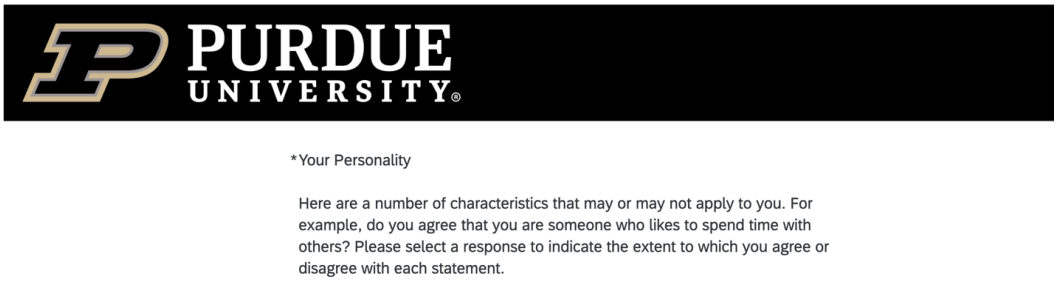


Figure C 1.

Instructions



APPENDIX D. PERSONALITY ASSESSMENTS

Table D1.

Descriptive Statistics for Big Five

Trait	Group 1 (*n* = 196) Mean (*SD*)	Group 2 (*n* = 61) Mean (*SD*)	Total (*n* = 257) Mean (*SD*)	Range (Min-Max)
Extraversion	3.05 (0.84)	3.01 (0.91)	3.04 (0.86)	1.25-5.00
Agreeableness	3.87 (0.62)	3.80 (0.66)	3.85 (0.63)	1.89-5.00
Conscientiousness	3.94 (0.64)	3.93 (0.74)	3.93 (0.69)	2.00-5.00
Neuroticism	2.59 (0.84)	2.69 (0.93)	2.61 (0.86)	1.00-4.88
Openness	3.72 (0.60)	3.96 (0.61)	3.78 (0.61)	1.30-5.00

Table D2.

Descriptive Statistics for Dark Triad

Trait	Group 1 (*n* = 196) Mean (*SD*)	Group 2 (*n* = 61) Mean (*SD*)	Total (*n* = 257) Mean (SD)	Range (Min-Max)
Machiavellianism	3.11 (0.74)	3.23 (0.76)	3.14 (0.74)	1.00-5.00
Narcissism	2.86 (0.64)	2.77 (0.77)	2.84 (0.66)	1.11-4.67
Psychopathy	2.20 (0.69)	2.18 (0.64)	2.20 (0.68)	1.00-3.89
Dark Triad Total	2.73 (0.49)	2.73 (0.57)	2.73 (0.51)	1.52-3.8889

Figure D1.

Big Five Inventory

How I am in general

Here are a number of characteristics that may or may not apply to you. For example, do you agree that you are someone who *likes to spend time with others*? Please write a number next to each statement to indicate the extent to which **you agree or disagree with that statement.**

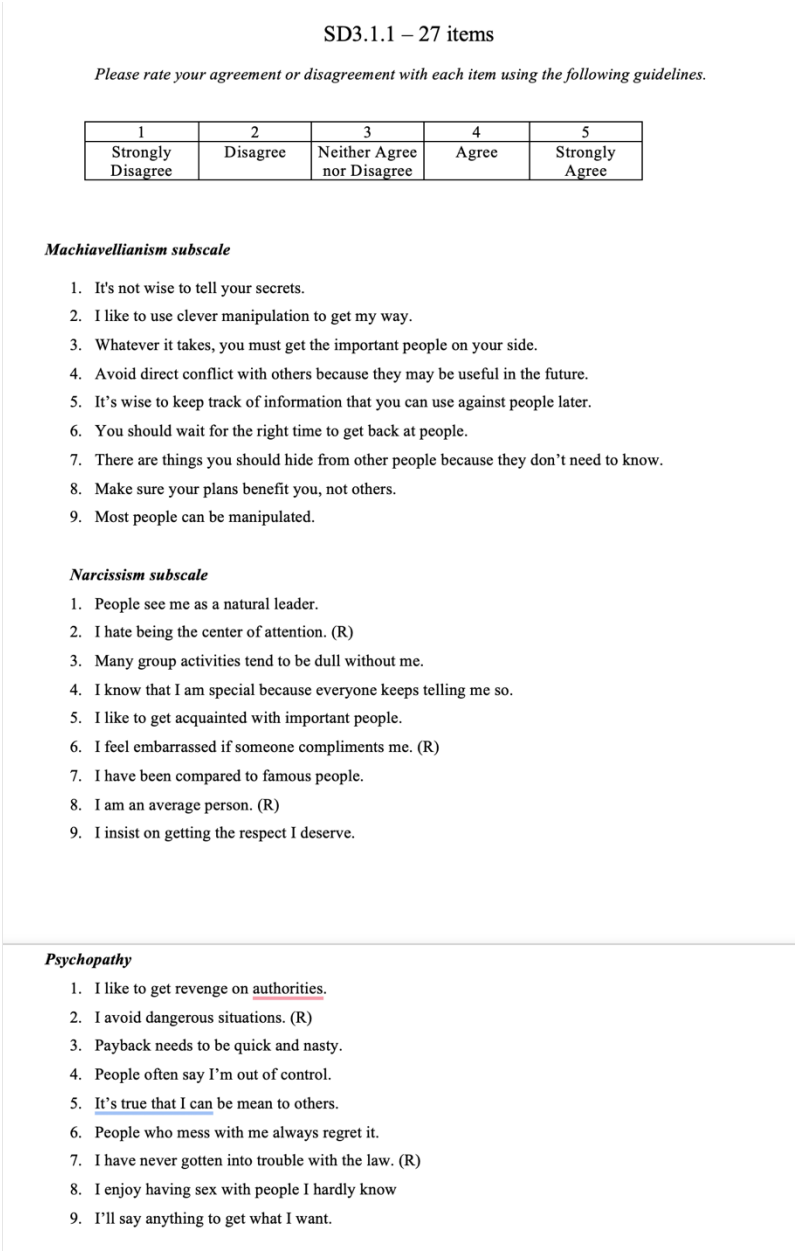
1 Disagree Strongly	2 Disagree a little	3 Neither agree nor disagree	4 Agree a little	5 Agree strongly

I am someone who…

1. _____ Is talkative
2. _____ Tends to find fault with others
3. _____ Does a thorough job
4. _____ Is depressed, blue
5. _____ Is original, comes up with new ideas
6. _____ Is reserved
7. _____ Is helpful and unselfish with others
8. _____ Can be somewhat careless
9. _____ Is relaxed, handles stress well.
10. _____ Is curious about many different things
11. _____ Is full of energy
12. _____ Starts quarrels with others
13. _____ Is a reliable worker
14. _____ Can be tense
15. _____ Is ingenious, a deep thinker
16. _____ Generates a lot of enthusiasm
17. _____ Has a forgiving nature
18. _____ Tends to be disorganized
19. _____ Worries a lot
20. _____ Has an active imagination
21. _____ Tends to be quiet
22. _____ Is generally trusting
23. _____ Tends to be lazy
24. _____ Is emotionally stable, not easily upset
25. _____ Is inventive
26. _____ Has an assertive personality
27. _____ Can be cold and aloof
28. _____ Perseveres until the task is finished
29. _____ Can be moody
30. _____ Values artistic, aesthetic experiences
31. _____ Is sometimes shy, inhibited
32. _____ Is considerate and kind to almost everyone
33. _____ Does things efficiently
34. _____ Remains calm in tense situations
35. _____ Prefers work that is routine
36. _____ Is outgoing, sociable
37. _____ Is sometimes rude to others
38. _____ Makes plans and follows through with them
39. _____ Gets nervous easily
40. _____ Likes to reflect, play with ideas
41. _____ Has few artistic interests
42. _____ Likes to cooperate with others
43. _____ Is easily distracted
44. _____ Is sophisticated in art, music, or literature

Figure D2.

Short Dark Triad Scale



SD3.1.1 – 27 items

Please rate your agreement or disagreement with each item using the following guidelines.

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Machiavellianism subscale

1. It's not wise to tell your secrets.
2. I like to use clever manipulation to get my way.
3. Whatever it takes, you must get the important people on your side.
4. Avoid direct conflict with others because they may be useful in the future.
5. It's wise to keep track of information that you can use against people later.
6. You should wait for the right time to get back at people.
7. There are things you should hide from other people because they don't need to know.
8. Make sure your plans benefit you, not others.
9. Most people can be manipulated.

Narcissism subscale

1. People see me as a natural leader.
2. I hate being the center of attention. (R)
3. Many group activities tend to be dull without me.
4. I know that I am special because everyone keeps telling me so.
5. I like to get acquainted with important people.
6. I feel embarrassed if someone compliments me. (R)
7. I have been compared to famous people.
8. I am an average person. (R)
9. I insist on getting the respect I deserve.

Psychopathy

1. I like to get revenge on authorities.
2. I avoid dangerous situations. (R)
3. Payback needs to be quick and nasty.
4. People often say I'm out of control.
5. It's true that I can be mean to others.
6. People who mess with me always regret it.
7. I have never gotten into trouble with the law. (R)
8. I enjoy having sex with people I hardly know
9. I'll say anything to get what I want.

APPENDIX E. SCENARIO

<table>
<tr><th colspan="2">Scenario Overview: Penetration Testing a Large Regional Hospital</th></tr>
<tr><td colspan="2">Background:
You are conducting a penetration test against a large regional hospital in the Midwest USA during peak sickness season (winter). The hospital is a multi-location facility serving a metropolitan area and has over 14,000 employees, including doctors, nurses, IT staff, and administrative personnel. It is also affiliated with an academic medical center, meaning it supports research, teaching, and clinical trials.

Technology & Infrastructure:
• The hospital runs primarily on Windows-based machines, but IT and cybersecurity teams use MacOS.
• The cybersecurity team consists of six analysts, while IT has 10 specialists.
• Some IT and security functions are outsourced to a Managed Service Provider (MSP).
• BYOD (Bring Your Own Device) is allowed for accessing certain medical software and emails, especially for traveling doctors and nurses.
• The hospital encourages the use of Chrome but does not strictly monitor which browsers employees install.
• Some machines (e.g., surgical equipment, patient monitoring systems) are on a closed network, requiring a staff key fob for access. Some endpoints have limited internet connectivity.
• The hospital is currently overwhelmed with 500+ ER patients per day, leading to strained resources and overworked staff.</td></tr>
<tr><th colspan="2">Inject 1: Reconnaissance</th></tr>
<tr><td>Information: It is peak flu/RSV/COVID season. The hospital is overwhelmed, and staff are exhausted. Security vigilance is lower than usual due to the crisis. You are preparing your attack.</td><td>Open-ended question:
What reconnaissance steps do you take, and how do you prioritize targets given the high-traffic, high-stakes environment?</td></tr>
<tr><th colspan="2">Inject 2: Initial Access</th></tr>
<tr><td>Information: Through OSINT and scanning, you’ve discovered multiple unpatched vulnerabilities and outdated operating systems. Hospital staff are receiving hundreds of emails per day, making them susceptible to phishing.</td><td>Open-ended question:
“What is your primary method to maintain access while avoiding detection?”</td></tr>
<tr><th colspan="2">Inject 3: Evasion & Persistence</th></tr>
<tr><td>You’ve successfully breached the network. However, the hospital’s security team and MSP monitor network activity. You need to evade detection.</td><td>Open ended question:
“Now that you have access, how do you maintain persistence while minimizing detection from security tools and the MSP?”</td></tr>
<tr><th colspan="2">Inject 4: Expanding Access & Escalation</th></tr>
<tr><td>You now have persistence and are exploring higher-value targets.

You realize:
• The hospital stores patient records (PHI) on a separate internal database.
• Scheduling and medication dispensing systems are critical to daily operations.
• The hospital relies on its MSP for patching and security monitoring.</td><td>Closed and Open-ended question:
“Which target do you choose and why?”

1. Electronic Health Records (EHR) database (PHI theft).
2. Hospital scheduling & medication systems (operational disruption).
3. MSP access (to escalate to broader systems).</td></tr>
<tr><th colspan="2">Inject 5: Detection & Incident Response</th></tr>
<tr><td>Your activity triggers an alert, and the hospital’s SOC (Security Operations Center) and MSP begin investigating. The hospital is considering shutting down segments of the network.</td><td>Open-ended question:
“You suspect security teams are onto you. How do you adapt your strategy to continue operating without getting caught?”</td></tr>
<tr><th colspan="2">Inject 6: Ransomware Deployment or Exit Strategy</th></tr>
<tr><td>At this point, you have two major options:
1. Deploy ransomware to lock systems and demand payment.
2. Exfiltrate valuable data and exit quietly.</td><td>Close-ended question:
“Would you prioritize deploying ransomware (locking hospital systems) or stealing data (exfiltration)?

• (A) Ransomware—because it maximizes immediate disruption and forces payment.
• (B) Data exfiltration—because PHI can be sold on the black market and reused.</td></tr>
</table>

APPENDIX F. EXTENDED RESPONSES

Extended Intrusion Strategy: Single Participant Example

Example multi-step direct response from one participant.

Reconnaissance Steps:

1. Passive Reconnaissance (Priority #1 – Stealth First):
    - OSINT Gathering: Scan public-facing resources (website, job listings, social media, staff LinkedIns, press releases) for tech stack, vendors (e.g., EMR systems like Epic/Cerner), IP ranges, VPN use, remote access policies, and staff behaviors.
    - Shodan/Censys Searches: Identify exposed hospital infrastructure (e.g., remote desktop services, unpatched medical IoT devices).
    - WHOIS & DNS Records: Enumerate domains and subdomains to map the hospital's digital footprint.
2. Network & Infrastructure Mapping (Priority #2 – Entry Identification):
    - Use tools like nslookup, dig, or sublist3r to enumerate subdomains.
    - Conduct passive scanning with theHarvester or Recon-ng to identify emails, hosts, and third-party vendors.
    - Identify external IPs tied to VPN portals, OWA, Citrix, or telehealth platforms that may be misconfigured or under-protected.
3. Human Intelligence & Behavioral Recon (Priority #3 – Social Engineering Prep):
    - Monitor staff activity on social media or in public forums. Staff exhaustion can lead to risky behavior (e.g., oversharing or reusing passwords).
    - Identify likely targets for phishing: help desk, nurses, admin staff—especially those with elevated access who may be overwhelmed and more likely to click.

4. Physical Recon (Low Priority but Contextual):
    - If this were a red team scenario involving onsite engagement, observe entrances/exits, badge behavior, and any unattended terminals or access points.
    - Monitor trash for improperly discarded paperwork or credentials (Dumpster Diving), though this is usually outside of digital-only scope.

Prioritization of Targets:

1. Remote Access Portals (Highest Risk + High Utility):
    - VPNs, Citrix, webmail, and RDP portals are often misconfigured or exposed, especially during emergencies.
2. High-Access Users (Next-Highest):
    - IT staff, billing admins, and senior medical personnel (e.g., CMO or chief radiologist) often have wide access and are overwhelmed.
3. Medical IoT Devices and Legacy Systems (Vulnerable Targets):
    - Many hospitals run outdated devices or Windows systems without updates, making them easy to fingerprint and exploit.
4. Third-Party Vendors & Supply Chains:
    - Look for vendors or contractors (especially temporary staffing or medical supply platforms) that may use weak authentication or lack hardened protocols.

Strategic Considerations Given the Crisis:

- Exploit Shifted Priorities: Staff are focused on patient care, not security—phishing and Social Engineering are more likely to succeed.
- Stay Quiet, Stay Watching: Let chaos expose vulnerabilities—your job is to listen, gather, and wait for the right time to exploit low-hanging fruit.

- Avoid Denial of Service: In a real-world ethical red team, do not perform noisy scans or actions that could impair already-overwhelmed systems.

Single Sophisticated Intrusion Response

“First step is always to perform passive recon. So I'd map out the website and any subdomains. From there, you can do some additional information gathering by looking at any job postings they have and seeing what skills they're looking for. This will give you some insight as to what software and technologies they are using. You can also use Linkedin and social media to gather names of employees that work there so stage some Social Engineering attacks. the next phase would be some network probing. I'd want to generate a map of their outer perimeter and then check for known vulnerabilities. I'm guessing that there are some remote access portals as well as some vendor remote support portals. Those could be good targets. Let's get a list of potential vendors. Perhaps they're using default credentials. Something to think about for later. For now, let's focus on the human element and start with some phishing. Craft an email that will get some attention. Peak COVID season, so that could be a good hook. Perhaps attach a PDF that contains an exploit, or include a hyperlink to a crafted site with some malicious code that can take over their browser. So the goal is to penetrate the network, and not to disrupt operations. This is a healthcare facility, and you don't want to put lives at risk. But you do want to show that they are vulnerable. Have to tread lightly without being disruptive. Get inside the network, perform mapping, gain admin credentials, secure pivot points, compromise critical systems such as HR, payroll, EHR, remote access systems, messaging platforms, and all databases. Take a structured approach. Know and understand what types of defenses they have and how to avoid them. Cover all of your

tracks and remain undetected. C-Level executives can be very prone to phishing, and they usually have high and undeserved levels of access to most systems.

…MSP? Music to my ears. Most MSP's promise way more than they can actually deliver. They advertise having stacks of security monitoring tools that their staff isn't trained to use. So they get bombarded with alerts that they eventually end up ignoring. So this is key knowing that there could be some potential bling spots. Let's find out who the MSP is. Visit their website and see what services they offer. Perhaps I can perform some misdirection to keep them busy if I'm concerned with my main attacks being noticed. But if stealth is the primary goal, perhaps it would be best to go after the monitoring agents. Not an easy task assuming that every system has an agent. This vector could create a lot of noise. However if successful, you'll have complete ownership. Might be worth the effort. We'll need a copy of the agent they're using to practice on in a virtual environment. That aside, already having access and being undetected is a huge plus. We've managed to be evasive so far and go undetected. Don't do anything that will create a lot of noise or raise eyebrows."

Structured and Reconnaissance Behaviors: Multiple Participant Excerpts

"I'd start by mapping everything I can. Know the environment before making a move."
"In a high-traffic, high-stakes environment, reconnaissance must be both strategic and efficient. The process typically begins with passive reconnaissance, gathering publicly available information (OSINT) such as domain names, IP ranges, employee details, and exposed services without alerting the target. Tools like WHOIS, Shodan, and Google Dorking are useful here. Once a baseline is established, active reconnaissance follows, using tools like Nmap or Nessus to map the network, identify live hosts, open ports, and potential vulnerabilities."
"I'd check configurations and user permissions before running anything. There's no reason to be sloppy."
"First, I'd do some passive recon—check the hospital's website, LinkedIn, and job boards to see what tech they use and who works there. I'd look for emails, vendor names, and any signs of old or unpatched systems. Since the staff's stressed and tired, I'd go after people using their own devices first—like traveling doctors or nurses. They're more likely to click something. I'd also check for remote access stuff like VPNs or MSP logins. Main targets would be IT folks or researchers—they probably got the most access and maybe not much security around them right now."