

The relationship between the dark triad personality and cybersecurity

Péter Bányász

Department of Cybersecurity, Ludovika University of
Public Service, Hungary
banyasz.peter@uni-nke.hu

Tamás Szádeczky

Department of Cybersecurity, Ludovika University of
Public Service, Hungary
szadeczky.tamas@uni-nke.hu

Pál K. Laska

Doctoral School of Military Engineering, Ludovika
University of Public Service, Hungary
laska.pal@mailfence.com

Kincsó B. Vácz

John Lukacs Institute for Strategy and Politics, Ludovika
University of Public Service, Hungary
vaczi.kincso.boroka@uni-nke.hu

ABSTRACT

The current study endeavors to explore the linkages between the Dark Triad personality traits, namely narcissism, Machiavellianism, and psychopathy, and the attitudes towards cybersecurity among university students who are registered in an information security awareness course. The research involved administering a self-report questionnaire to 29 students that included queries on the Dark Triad personality scale and cybersecurity attitudes. The research will use a mixed-methods approach to analyse the data, including quantitative such as descriptive statistics, cross-tabulation analysis, cluster analysis. The findings of this study may offer insights that could aid in the development of customized information security training programs and the enhancement of cyber threat management.

CCS CONCEPTS

• **Security and privacy** → Human and societal aspects of security and privacy; Social aspects of security and privacy; Human and societal aspects of security and privacy; Social aspects of security and privacy; • **Applied computing** → Law, social and behavioral sciences; Psychology.

KEYWORDS

Cybersecurity Awareness, Dark Triad, Survey

ACM Reference Format:

Péter Bányász, Pál K. Laska, Tamás Szádeczky, and Kincsó B. Vácz. 2024. The relationship between the dark triad personality and cybersecurity. In *Central and Eastern European eDem and eGov Days 2024 (CEEeGov 2024)*, September 12, 13, 2024, Budapest, Hungary. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3670243.3670262>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CEEeGov 2024, September 12, 13, 2024, Budapest, Hungary

© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-1709-3/24/09
<https://doi.org/10.1145/3670243.3670262>

1 INTRODUCTION

The advent of Information and Communication Technologies (ICTs) has significantly altered the security risks, often introducing unprecedented types of risks that are particularly relevant to the public sector. Students enrolled at the Ludovika University of Public Service hold a unique position in this regard, as they are likely to pursue careers in public administration, law enforcement, defense, or national security organizations upon graduation - or may already be employed in one of these organizations as correspondence course students. Subsequently, it is of paramount importance for education to assume a crucial role in ensuring that students acquire adequate data and information security awareness.[2] Nevertheless, the education sector has experienced numerous transformations, and educators encounter similar challenges irrespective of the subject matter. The delivery of information security training demands meticulous attention to detail, primarily because students can get easily distracted by smart mobile devices, making it challenging to sustain their attention. This predicament is further compounded if the course is scheduled in the evening, as students typically spend the entire day attending classes and are already fatigued. Consequently, despite the presence of interest in the subject matter, the workload can impede the ability to concentrate on what is being taught in class. It is important to acknowledge that some students may not exhibit any interest in the course content and may only be motivated by the desire to obtain credits or complete the course. Notably, contemporary teaching approaches rely heavily on conventional tools such as formal didactic teaching, personal mentoring, workshops, and modular learning materials. However, it is discernible that there is a requirement for more individualized teaching aids, which must encompass moral and ethical considerations in the evaluation process. This distinction is particularly relevant in the case of ethical hacking in comparison to cracking.

Over the past few decades, numerous studies have identified correlations between personality traits, internet use patterns, and information security awareness.[21] [9] [27] For instance, Alexander Kogan based Cambridge Analytica's services on the Big Five personality types.[8] [17] The Big Five personality model sorts individuals into five distinct factor groups - extraversion, agreeableness, conscientiousness, openness, and neuroticism or emotional stability - based on specific characteristics identified through factor analysis.[23] Our actions on Social Networking Sites, such as our likes, music preferences, and shared content, contribute to the platforms'

algorithms profiling us. Extensive research has been conducted on the correlation between Facebook activity and an individual's personality, which has shown that it is feasible to establish a link between likes and personality using the Big Five personality model. [15] [13] [4]

Personality traits also play a crucial role in developing information security messages and training programs. [29] [18] [26] To ensure that different personality types not only have a comprehensive understanding of different security standards but also integrate them into their r, tailored messages should be crafted for each type. Password management provides a pertinent example of this, as many users are aware of the basic principles of good password creation practices, yet they do not put them into practice. Consequently, the message conveyed in an information security awareness training course should not be the same for all. One approach that can be adopted is the Deterrence Theory, which Gibbs developed in 1975. The theory is based on an individual's cost-benefit perspective, where they aim to maximize gains and minimize losses. The theory highlights the role of formal sanctions, which are more effective when they are severe and larger in size. [11] [16] [28]

Morality is another approach that can significantly influence an individual's decision-making through the transmission of ethical messages. Studies indicate that this approach is also relevant in the context of information security. [22] [14] A noteworthy message in this regard is regret, which is premised on an individual's ability to evaluate the consequences of their decisions. Avoidance of expected negative consequences serves as a suitable incentive. Regret has a significant impact on an individual's thinking and behavior. [1] [12] [30] In the context of information security, regret-based messages effectively influenced some behaviors, such as backing up, but not security-conscious internet use. Few studies have investigated the role of incentives in information security, but they have established a correlation between incentives and security-conscious behavior [3] [7] [24], albeit one that is not very strong [6]. Finally, feedback may be used as a message. Feedback can be viewed as an extension of deterrence, where negative feedback discourages bad practices, and positive feedback reinforces desirable behavior. Research has shown that socially relevant issues, such as selective waste collection, are effective, but the results are inconclusive when it comes to information security awareness.

In psychology, the concept of the "dark triad" (DT) encompasses three malevolent personality traits: narcissism, Machiavellianism, and psychopathy. Over the past 15 years, there has been an increasing interest among scholars in studying "dark behaviors" and "dark traits," particularly in organizational contexts. The DT represents a taxonomy of dark personality traits that have undergone extensive examination, with researchers attempting to comprehend how these traits relate to other personality models (such as the Five Factor Model or Big Five) and to various organizationally relevant processes and outcomes (such as counterproductive workplace behaviors and leadership). James and LeBreton defined personality as "dynamic mental structures (e.g., scripts, schemas, motives, needs) associated with mental processes (e.g., perceiving, framing, encoding, analyzing, inferring) that determine an individual's cognitive, affective, and behavioral adjustments to his or her environments." The authors further distinguished between the implicit and explicit

components of personality, with the former referring to the aspects of personality that exist beyond conscious awareness (such as defense mechanisms) and the latter referring to the aspects of personality that one is consciously aware of (such as introspectively accessible thoughts, feelings, and patterns of behavior). Thus far, the majority of research, both in general and in the organizational sciences, has focused on the explicit components of the DT, primarily in the form of explicit traits. Given this, our review will concentrate on those aspects of the DT that are accessible to introspection and are most frequently measured through self-report surveys.

The present study employs the Dark Triad construct [25] [19] [10], which encompasses Machiavellianism, subclinical narcissism, and subclinical psychopathy, to explore the domain of cybersecurity awareness. While the term "subclinical" refers to the absence of readily detectable clinical symptoms and is commonly used for diseases that lack manifest symptoms at an early stage, we have omitted the term for simplicity, while still refraining from referring to narcissism or psychopathy in the clinical sense. Although the members of the Dark Triad exhibit several commonalities, they possess distinct characteristics, which is why they have been grouped together as a triad. Machiavellianism is the only member of the Dark Triad that lacks a psychopathological counterpart or a diagnosed level of severity. The phenomenon associated with Machiavellianism varies across disciplines, with the term being widely associated with political sciences. However, in the narrower psychological sense, Machiavellianism was first discussed in more detail during the 1970s. Machiavellians prioritize their objectives over the benefit or harm of others, manipulating without regard for ethical considerations. They are cynical and suspicious, believing that if they do not take advantage of others, they will be taken advantage of themselves. While they do not consider their interests superior to those of others, they are not altruistic and emotionally withdraw from situations. Machiavellians possess the ability to understand the thoughts and intentions of others, but lack emotional involvement or empathy with the characters in the story. They are skilled strategists who prioritize the interests of their own group. Machiavellianism, despite not being classified as a type of psychopathy, is increasingly being debated as a subclinical form of the latter. Furthermore, its lack of empathy has led it to be considered a subclinical form of sociopathy.

The concept of narcissism was introduced by Freud and distinguished between 'normal' or primary narcissism and pathological or secondary narcissism. While Freud's theory on narcissism was criticized, contemporary approaches still view narcissism as a developmental process rather than just pathological. However, several authors have posited that poor parental care, particularly the lack of or damage to early emotional attachments, is the root cause of narcissistic pathology. Such caregiver dysfunctions during early childhood have a significant impact on one's self-development.

The roots of psychopathy can be traced back to the early 1800s. However, over time, descriptions of this condition have varied widely, ranging from reckless and impulsive behavior associated with intact mental faculties to a charming, persuasive, confident, attention-seeking, and emotionally shallow nature, as well as emotional coldness, callous exploitation of others, and brutality. These

diverse early conceptualizations demonstrate the controversial nature of psychopathy's definition. The most widely recognized division of psychopathy is the two-factor model, which differentiates between primary and secondary psychopathy. Primary psychopathy is attributed to an innate emotional deficit, characterized by low anxiety levels and a subsequent antisocial behavior, a lack of guilt, and an inability to recognize and learn from mistakes, as well as underactivity of the behavioral inhibitory system. Secondary psychopathy, on the other hand, is a personality constellation acquired as a result of adverse environmental influences, where increased exposure to anxiety, abuse, neglect, or emotional coldness and the resulting negative experiences and feelings lead to increased anxiety, emotional distress, and antisocial behavior in response to emotional distress and intrapsychic conflict. In this case, the behavioral activation system is in overdrive. In addition to their innate emotional deficit, primary psychopaths are characterized by extroverted behavior, greater openness, and confidence, which stem from their lower anxiety levels. Conversely, secondary psychopaths exhibit the opposite traits, including emotional disturbance, decreased social activity, and increased impulsivity.

The Dark Trinity, consisting of three constructs, is typified by manipulative behavior, self-interest, emotional coldness, and heightened levels of aggression, which often elicits a negative connotation. However, these constructs are not classified as psychopathologies, and they share common features such as self-centeredness and reduced empathy, which are more prevalent in men. Despite this, not all members of the Dark Trinity exhibit the same characteristics, leading to debates about treating them as a single entity or as separate constructs. While the Dark Trinity's traits are correlated, they are not interchangeable, and their degree of expression may vary from person to person. The constructs overlap in their common intersection of self-interest, manipulation, and insensitivity, but they also have distinctive features that differentiate them from each other. The Dark Trinity's individual characteristics can be discerned through the prevailing structural models of personality, such as the Interpersonal Circle or the Big Five model.

2 METHODOLOGY

Our research was conducted within the framework of two optional courses, which are generally open to undergraduate students, with the exception of one Master's degree program. The first course, "Information Security Awareness," was offered in the first semester of 2023/2024, while the second course, "The Regulation of Privacy, Public Security and Surveillance," was offered in the second semester of 2023/2024. Full time training students attended the daytime classes (24 people), which totaled 28 hours over 14 weeks on Monday evenings from 6:00 pm, while part time training classes (5 people) were held for 2x4 hours. The participants of the experiment were drawn from various degree programs, with the course offered in two faculties of the University. The International Security and Defense Policy course (3 people) was provided to students enrolled in the Faculty of Military Sciences and Officer Training, while students enrolled in the Faculty of Public Governance and International Studies were offered the other courses, Public Administration Manager (8 people), Science of Public Governance (14 people), International Public Management courses (4 people).

The majority of the participants took the course as an elective for their degree, with only a small percentage demonstrating a genuine interest in the subject matter. The 6:00 pm start time of the course played a crucial role in motivating the students, as the challenges outlined earlier were formulated. Notably, 19 of the students had previously completed one of the two courses in an earlier semester.

In the first session of the course, we conducted a focus group survey to assess the information security awareness of students, utilizing the five-step information security awareness model.[5] We queried students on their knowledge, attitudes, legal knowledge, intentions, and behaviors.

Finally, with regards to behavior, we inquired about the protection measures employed on their devices.

The results were remarkable, albeit not unexpected. The participants' attitudes towards safety awareness centered on conventional responses such as "I am not a noteworthy target," "I am not intrigued by the subject," and "I am not technically inclined, hence the subject is not of interest to me." The mainstream media's coverage of cybersecurity has only captured my attention superficially, if at all.

To overcome the aforementioned challenges of indifference and fatigue, we employed a novel teaching methodology known as "comedication" program.[20] This program was initially introduced in medical education, with the first program comprising short videos in 1994; however, the authors have since expanded it to include cinema and episodes of television series. Film is an effective medium for presenting diverse forms of cyberspace behavior, as it simplifies complex issues, offers multiple potential solutions, and can serve as a case study to prepare students for real-life situations. "Cinemedication" has proven to be an effective and engaging tool for evaluating professionalism while also promoting critical thinking and moral maturity. The utilization of film illustrations in education is widespread and has been a tried and tested method in history, philosophy, and political science. This approach permits a comprehensive exploration of a phenomenon from various perspectives - in public service, it is crucial to consider not only the interests of the average user but also the state's defense mechanisms, as well as the legal regulations involved. To gauge individual progress in each lesson, we employed a gamification-based application called Kahoot. At the outset of each lesson, we created a quiz related to the topic, examining general knowledge to assess the participants' baseline knowledge. Conversely, at the end of each lesson, we formulated a quiz consisting of specific questions that tested knowledge covered during the session. This approach aimed to evaluate competencies while measuring the degree of student engagement. The Kahoot test demonstrated, lesson by lesson, that this innovative approach managed to sustain student interest and attention, even when they were fatigued from attending classes throughout the day. While the general Kahoot test at the beginning of the course yielded mixed results, a significant proportion of students provided correct answers to the specific knowledge covered in each lesson. Feedback from students at the end of the course corroborated our assumptions: not only had their awareness levels increased, but their behavior had also transformed in numerous instances, with some referencing a common phrase, "I have covered my webcam since then".

Table 1: The 14-week course encompassed the following topics related to cybersecurity

Week	Information security awareness	The Regulation of Privacy, Public Security and Surveillance
1	Introduction to the information security awareness	Introduction to the privacy
2	Social Engineering I.- Human-based attacks	The legislation of the privacy, public security and surveillance
3	Social Engineering II.- IT-based attacks	The legislation of video surveillance. Intelligent video surveillance
4	Cyber threats I.- Cyber crime	The legislation of the public video surveillance (Police, Department of Streets, public transport)
5	Cyber threats II.- Cyber terrorism and hacktivism	The Big Brother and the Surveillance Society
6	Cyber threats III.- Cyber espionage	Smartphone surveillance and tracking techniques
7	Cyber threats IV.- Cyber warfare	Deep Packet Inspection
8	Psychological operations	The benefits and challenges of UAVs
9	The risks of social media	Biometric authentication
10	Cyberbullying	The Right to be forgotten. 2018 reform of EU data protection reform
11	The safety of smart mobile devices	Using technology to protect Online Privacy. Privacy Enhancing Technologies, Privacy by Design
12	Best practices in building information security awareness	Best practices in data privacy
13	Presentations	Presentations
14	Conclusion	Conclusion

Subsequent to implementing this educational methodology, we administered a questionnaire to the students at the midpoint of the semester, which assessed the relationship between cybersecurity and the dark triad personality test. As previously mentioned, a total of 29 students participated across both semesters; hence, we cannot make generalizations beyond the respondents' valid results. There exists a multitude of versions of the Dark Triad test, however, for our study, we employed the abbreviated version consisting of 27 items for each of the three factors. In addition to the fundamental set of questions, we included two supplementary sets of inquiries that could be classified under two factors, namely, perception and cybersecurity awareness. The aforementioned constructs were evaluated using a Likert scale, with the Dark Triad questions being measured on a scale of 1 to 5 and the cybersecurity questions on a scale of 1 to 4. Further, we subdivided the cybersecurity constructs based on knowledge and attitudes, in which 4 and 15 questions were asked, respectively. Lastly, we assessed two questions on perception.

Owing to the limited number of responses to the questionnaire, we employed certain methods to validate the questionnaire. Our analyses were conducted using descriptive statistics, cluster analysis, and the Kruskal-Wallis test.

The purpose of our research is to explore the correlations between cybersecurity awareness and the responses of the participants to the Dark Triad questionnaire.

The following hypotheses are related to this study:

H1: Respondents are predominantly characterized by narcissistic traits rather than Machiavellian or psychopathic traits.

H2: Respondents who consider themselves security-conscious will display a greater sense of responsibility towards preventing incidents.

H3: Respondents who consider themselves security-conscious are perceived to be more comfortable with rules and less vulnerable than their non-security-conscious counterparts.

3 RESULTS

The responses received for the Dark Triad test were subject to analysis using descriptive statistics on a sample size of 29. The results show that the highest mean score for Machiavellianism was 4.55 ("There are things you should hide from other people to preserve your reputation"), which although did not score a tick in this category, was the highest mean score among all 27 questions. This finding suggests that Machiavellianism is a prominent factor amongst the respondents. It is noteworthy to mention that the category of Machiavellianism also had the highest mean value of the standard deviation (1.088), indicating a wide range of responses. In contrast, the lowest value was recorded for psychopathy ("I like to pick on losers" =1.38), with this category also having the lowest average standard deviation among all questions (1.027). Upon averaging the responses for each question, the results reveal that Machiavellianism has the highest value (3.59).

Comparable to the Dark Triad test, descriptive statistics were employed to analyze the responses received for questions pertaining to cybersecurity knowledge and attitudes. Given that the responses were measured on a 1 to 4 scale, the mean for both factors slightly exceeded the median.

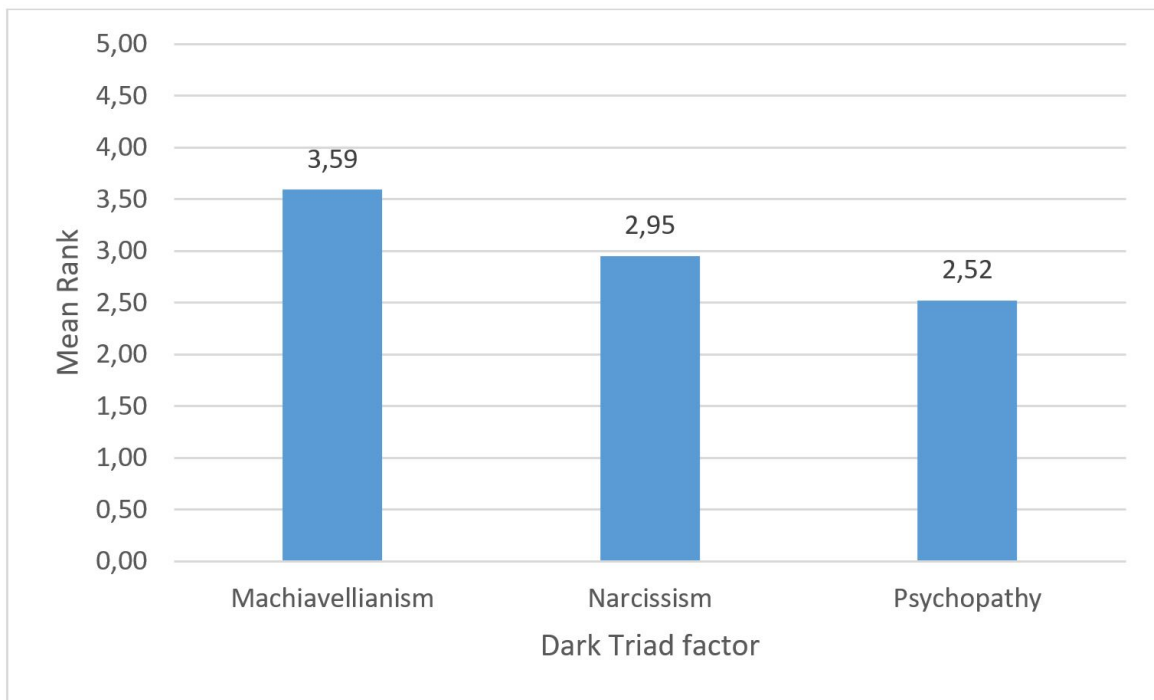


Figure 1: Mean scores of the respondents on the Dark Triad's factors (own editing, N=29)

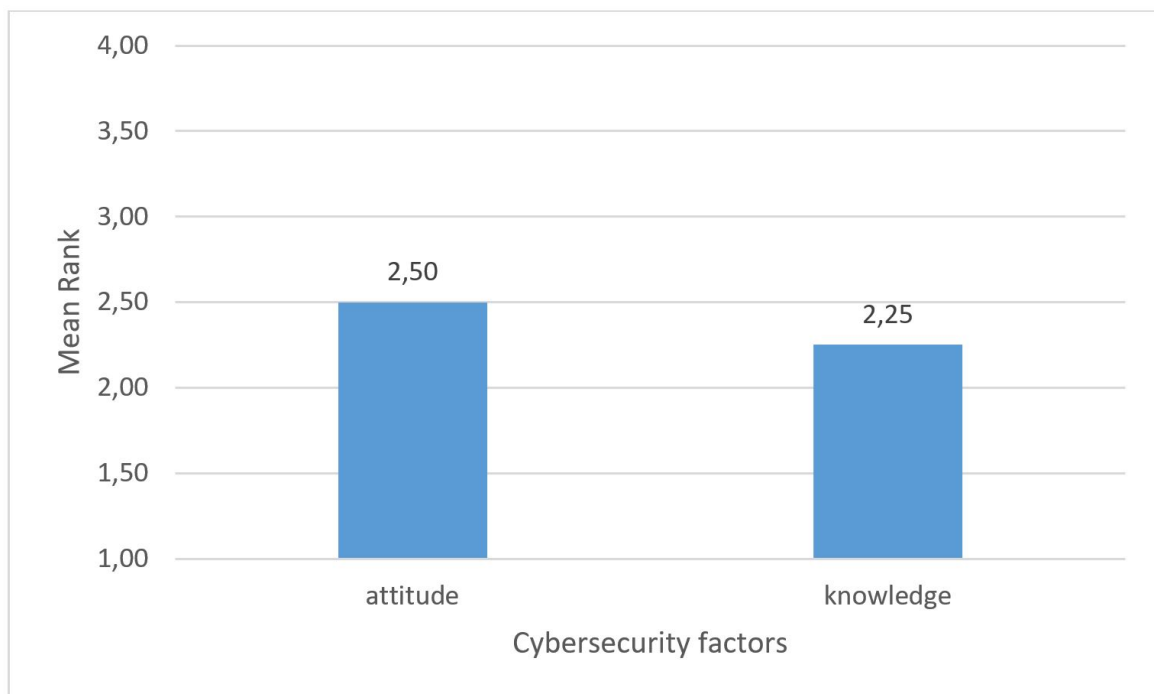


Figure 2: Mean scores of the respondents on the Cybersecurity factors (own editing, N=29)

Following this, we proceeded to conduct a cluster analysis for the three-factor questions of the Dark Triad test. Initially, we analyzed the responses to the questions relating to Machiavellianism using Ward's Method, which yielded two clusters based on the dendrogram:

1. Stronger Machiavellianism: In this group, five out of the nine questions exhibited a higher mean score, indicating that the respondents may possess a higher tendency towards Machiavellianism traits.

2. Moderate Machiavellianism: Although some questions had high mean scores, they were less concentrated and lower for some questions, indicating a more moderate tendency towards this factor.

Subsequently, we formed clusters based on the responses to the narcissism questions utilizing Ward's method, similar to the Machiavellianism method. Herein, the two-cluster separation was again the most optimal:

1. Intense narcissism: In this group, five out of the nine questions exhibited a higher mean score, which may indicate a more intense display of narcissistic traits among respondents.

2. Broad spectrum of narcissism: Although the average score for four questions was higher in this group, there was a higher deviation in three of these questions, suggesting a greater variety of responses and a broader spectrum of narcissistic traits among respondents.

In the final step, we formed two clusters based on the responses to the psychopathy questions using Ward's method, with the dendrogram and the values indicating that the two-cluster solution was appropriate:

1. High-intensity respondents: This group had a higher mean score for seven out of nine questions, with the deviation taking on different values for each response. The high scores in this group may indicate a stronger manifestation of psychopathy traits.

2. Balanced respondents: Two out of nine questions had a higher average score in this group. The degree of deviation differed across responses, but for the statement "I like to pick on losers," the deviation was 0, indicating that everyone gave the same answer to this question in this group.

As a further step in our research, we conducted the Kruskal-Wallis test to examine whether there were significant differences between groups based on specific variables. All three components of the Dark Triad were tested, and groups were formed based on the individual's perception of their security consciousness regarding privacy. Among the questions analyzed, there was a significant difference between those who considered themselves security conscious and those who did not, in the psychopathy question "I like to pick on losers". The significance level was $P=0.014$, indicating that those who did not consider themselves security conscious tended to agree more strongly that they liked picking on losers. However, for the questions in the Machiavellianism and Narcissism domains, there was no significant difference between the two groups for any of the questions asked.

Furthermore, using the Kruskal-Wallis test, we examined responses to questions related to cybersecurity attitudes and knowledge factors and tested these against two questions, "Have you previously taken a course on data and information security?" and "Do you consider yourself security aware from a data protection perspective?". The answers to these questions were used to form

two groups, and we investigated whether there were any significant differences between these groups in terms of their attitudes and knowledge towards cybersecurity.

Regarding attitudes, respondents who considered themselves security-conscious scored significantly higher on the following questions:

- "I believe that it is the responsibility of the management to ensure that the university protects itself from cybercrime" ($P=0.019$)
- "It is difficult to determine how to protect the university from cybercrime" ($P=0.012$)
- "I believe that reporting cybercrime is a futile exercise" ($P=0.013$)

Regarding knowledge, respondents who had previously taken a course on data and information security scored significantly higher ($P=0.002$) on the question "I lack the skills to protect the university from cybercrime" compared to those who had not taken such a course.

In addition to the question "Do you consider yourself to be security aware from a data protection perspective?" for perception, respondents who answered "no" had a significantly higher proportion of respondents who claimed to be aware of their role in protecting the university from potential cybercriminals ($P=0.029$). Similarly, regarding security awareness, those who did not consider themselves to be security aware were significantly more likely ($P=0.005$) than those who considered themselves security aware to declare that they were aware of the university's IT use policy and made efforts to comply with it.

4 DISCUSSION

The findings from this study contribute essential insights into the psychological traits and perceptions associated with security-conscious behavior. Three key observations were made which have significant implications for understanding individual differences in security awareness and responsibility.

Our first result reveals that participants predominantly exhibit Machiavellian traits rather than narcissistic or psychopathic traits. This is a crucial finding, suggesting that security-conscious individuals may employ cunning and strategic thinking, characteristic of Machiavellianism, in their approach to security and privacy. This may indicate a calculative and outcome-based approach to security, where decisions are made more based on expected benefits rather than ethical or communal considerations. Such traits could potentially influence the development of security policies that account for this strategic behavior, aiming to align individual and organizational security goals.

The second result presents a paradox where respondents, who consider themselves as security-conscious, do not necessarily feel a greater sense of responsibility towards preventing security incidents. This finding challenges the assumption that increased awareness and knowledge lead to responsible security behavior. It suggests that while individuals may be aware of security practices and consider themselves conscious of security, this self-perception does not directly translate into a proactive attitude towards security responsibilities. This discrepancy could be addressed in security training programs by not only increasing awareness but also fostering a sense of personal responsibility and impact among individuals.

Finally, our third finding that respondents who consider themselves security-conscious are perceived to be more vulnerable and less comfortable with rules than their non-security-conscious counterparts adds another layer of complexity. This could reflect a critical and questioning attitude towards existing security measures and a recognition of the limitations of such rules. The perception of vulnerability despite a high level of consciousness could also drive the need for more stringent personal and organizational security practices.

These findings open several avenues for future research. Further studies could explore the underlying reasons why security-conscious individuals feel vulnerable and their specific discomforts with security rules. Additionally, investigating the interplay between different dark triad traits (Machiavellianism, narcissism, and psychopathy) and security behaviors could yield more profound insights into how personality influences security policy compliance and the effectiveness of security interventions.

This study underscores the complexity of security consciousness and responsibility, revealing that the psychological profile of security-conscious individuals is not straightforward and is influenced by various traits and perceptions. The insights gained call for a nuanced approach to security education and policy-making, considering these diverse psychological aspects.

ACKNOWLEDGMENTS

TKP2021-NKTA-51 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme.

REFERENCES

- [1] Charles Abraham and Paschal Sheeran. 2004. Deciding to exercise: the role of anticipated regret. *Br J Health Psychol* 9, Pt 2 (May 2004), 269–278. <https://doi.org/10.1348/135910704773891096>
- [2] Noa Aharony, Dan Bouhnik, and Nurit Reich. 2020. Readiness for information security of teachers as a function of their personality traits and their assessment of threats. *Aslib Journal of Information Management* 72, 5 (January 2020), 787–812. <https://doi.org/10.1108/AJIM-12-2019-0371>
- [3] Terrence August and Tunay I. Tunca. 2004. Network Software Security and User Incentives. Retrieved April 27, 2024 from <https://papers.ssrn.com/abstract=1708220>
- [4] Danny Azucar, Davide Marengo, and Michele Settanni. 2018. Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. *Personality and Individual Differences* 124, (April 2018), 150–159. <https://doi.org/10.1016/j.paid.2017.12.018>
- [5] Bilal Khan. 2011. Effectiveness of information security awareness methods based on psychological theories. *Afr. J. Bus. Manage.* 5, 26 (October 2011). <https://doi.org/10.5897/AJBM11.067>
- [6] Scott R Boss, Laurie J Kirsch, Ingo Angermeier, Raymond A Shingler, and R Wayne Boss. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* 18, 2 (April 2009), 151–164. <https://doi.org/10.1057/ejis.2009.8>
- [7] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly* 34, 3 (2010), 523–548. <https://doi.org/10.2307/25750690>
- [8] David R. Carroll. 2021. Cambridge Analytica. In *Research Handbook on Political Propaganda*. Edward Elgar Publishing, 41–50. Retrieved April 27, 2024 from <https://www.elgaronline.com/edcollchap/edcoll/9781789906417/9781789906417.00010.xml>
- [9] Andrea Cullen and Lorna Armitage. 2018. A Human Vulnerability Assessment Methodology. In *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, June 2018. 1–2. <https://doi.org/10.1109/CyberSA.2018.8551371>
- [10] S.R. Curtis, P. Rajivan, D.N. Jones, and C. Gonzalez. 2018. Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior* 87, (2018), 174–182. <https://doi.org/10.1016/j.chb.2018.05.037>
- [11] John D'Arcy, Anat Hovav, and Dennis Galletta. 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* (March 2009). <https://doi.org/10.1287/isre.1070.0160>
- [12] Wilco W. van Dijk and Marcel Zeelenberg. 2002. Investigating the Appraisal Patterns of Regret and Disappointment. *Motivation and Emotion* 26, 4 (December 2002), 321–331. <https://doi.org/10.1023/A:1022823221146>
- [13] Mustafa Eşkişu, Rumeysa Hoşoğlu, and Kyler Rasmussen. 2017. An investigation of the relationship between Facebook usage, Big Five, self-esteem and narcissism. *Computers in Human Behavior* 69, (April 2017), 294–301. <https://doi.org/10.1016/j.chb.2016.12.036>
- [14] Russell Haines and Lori N. K. Leonard. 2007. Situational influences on ethical decision-making in an IT context. *Information & Management* 44, 3 (April 2007), 313–320. <https://doi.org/10.1016/j.im.2007.02.002>
- [15] Qiwei He, Cees A. W. Glas, Michal Kosinski, David J. Stillwell, and Bernard P. Veldkamp. 2014. Predicting self-monitoring skills using textual posts on Facebook. *Computers in Human Behavior* 33, (April 2014), 69–78. <https://doi.org/10.1016/j.chb.2013.12.026>
- [16] Tejaswini Herath and H Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18, 2 (April 2009), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- [17] Joanne Hinds, Emma J. Williams, and Adam N. Joinson. 2020. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies* 143, (November 2020), 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>
- [18] Nor Shahriz Abdul Karim, Nurul Hidayah Ahmad Zamzuri, and Yakinah Muhamad Nor. 2009. Exploring the relationship between Internet ethics in university students and the big five model of personality. *Computers & Education* 53, 1 (August 2009), 86–93. <https://doi.org/10.1016/j.compedu.2009.01.001>
- [19] James M. LeBreton, Levi K. Shiverdecker, and Elizabeth M. Grimaldi. 2018. The Dark Triad and Workplace Behavior. *Annual Review of Organizational Psychology and Organizational Behavior* 5, Volume 5, 2018 (January 2018), 387–414. <https://doi.org/10.1146/annurev-orgpsych-032117-104451>
- [20] Nuttha Lumlertgul, Naruchorn Kijpaisalratana, Nuttorn Pityaratstian, and Danai Wangsaturaka. 2009. Cinemeducation: A pilot student project using movies to help students learn medical professionalism. *Med Teach* 31, 7 (July 2009), e327–332. <https://doi.org/10.1080/01421590802637941>
- [21] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson. 2017. Individual differences and Information Security Awareness. *Computers in Human Behavior* 69, (2017), 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>
- [22] Liisa Myrsky, Mikko Siponen, Seppo Pahlila, Tero Vartiainen, and Anthony Vance. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* 18, 2 (April 2009), 126–139. <https://doi.org/10.1057/ejis.2009.10>
- [23] Warren T. Norman. 1963. Toward an adequate taxonomy of personality attributes: Replicated factor structure in peer nomination personality ratings. *The Journal of Abnormal and Social Psychology* 66, 6 (1963), 574–583. <https://doi.org/10.1037/h0040291>
- [24] Seppo Pahlila, Mikko Siponen, and Adam Mahmood. 2007. Employees' Behavior towards IS Security Policy Compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, January 2007. 156b–156b. <https://doi.org/10.1109/HICSS.2007.206>
- [25] Delroy L. Paulhus and Kevin M. Williams. 2002. The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality* 36, 6 (December 2002), 556–563. [https://doi.org/10.1016/S0092-6566\(02\)00505-6](https://doi.org/10.1016/S0092-6566(02)00505-6)
- [26] Gorana Rakić-Bajić and Vladimir Hedrih. 2012. Excessive use of the Internet, life satisfaction and personality factors. *Suvremena psihologija* 15, 1 (July 2012), 119–130.
- [27] Jordan Shropshire and Art Gowan. 2015. Characterizing the Traits of Top-Performing Security Personnel. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (SIGMIS-CPR '15)*, June 04, 2015. Association for Computing Machinery, New York, NY, USA, 55–59. <https://doi.org/10.1145/2751957.2751971>
- [28] Detmar W. Straub. 1990. Effective IS Security: An Empirical Study. *Information Systems Research* 1, 3 (September 1990), 255–276. <https://doi.org/10.1287/isre.1.3.255>
- [29] Jörg Uffen, Michael H. Breitner, Jörg Uffen, and Michael H. Breitner. 1AD. Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions. [https://services.igi-global.com/resolvedoi/resolve.aspx?doi=\\$10.4018/978-1-4666-8111-8.ch039](https://services.igi-global.com/resolvedoi/resolve.aspx?doi=$10.4018/978-1-4666-8111-8.ch039). Retrieved April 27, 2024 from <https://www.igi-global.com/gateway/chapter/www.igi-global.com/gateway/chapter/125323>
- [30] Chris Wright and Peter Ayton. 2005. Focusing on what might happen and how it could feel: can the anticipation of regret change students' computing-related choices? *International Journal of Human-Computer Studies* 62, 6 (June 2005), 759–783. <https://doi.org/10.1016/j.ijhcs.2005.03.001>