Revista de Educação e Pesquisa em Contabilidade
Journal of Education and Research in Accounting

Periódico de Publicação Contínua, digital e gratuito publicado pela Academia Brasileira de Ciências Contábeis | Disponível online em www.repec.org.br

REPeC, Brasília, v. 19, 2025 | DOI: http://dx.doi.org/10.17524/repec.v19.e3686 | ISSN 1981-8610

A look at narcissist traits, cybersecurity awareness, and breach costs: a study addressing students and professionals from the accounting field

Marcia Figueredo D'Souza
https://orcid.org/0000-0002-3196-5396

Juliana Ventura Amaral
https://orcid.org/0000-0001-7223-3848

Abstract

Objective: To analyze the influence of cybersecurity awareness and narcissistic personality traits on breach cost awareness.

Method: Descriptive research with a quantitative approach. Data were collected through a survey of two samples: 262 accounting students and 166 accounting professionals. Descriptive statistics and logistic regression were applied.

Results: Both students and professionals struggled with classifying breach costs and reporting them in financial statements. Cybersecurity awareness enabled professionals to understand the impacts of these costs better and feel more confident in their classification. Among students with stronger narcissistic traits, overconfidence led to reports of greater cybersecurity awareness; however, they failed to acknowledge their difficulties in classifying and reporting these costs. Professionals exhibited higher narcissistic scores and demonstrated greater knowledge in reporting breach costs in financial statements.

Contributions: The findings contribute to the literature, as empirical evidence on this topic remains limited, and offer practical implications for the professional field. They encourage reflection among companies and accounting education institutions on the need to develop specialized courses and content on cybersecurity, equipping accountants and aspiring accountants to recognize the financial impacts of cyberattacks.

Keywords: Cybersecurity awareness. Breach costs. Narcissism.

Published in Portuguese and English. Original Version in Portuguese.

Round 1: Received in 10/9/2023. Accepted on 9/2/2024 by Bruna Camargos Avelino, PhD PhD (Editor assistant) by Gerlando Augusto Sampaio Franco de Lima, PhD (Editor). Published on 3/31/2025. Organization responsible for the journal: Abracicon.

1 Introduction

Cybersecurity breaches present escalating risks as networked systems and the Internet become increasingly pervasive. This growing threat requires greater attention to the accounting implications of attacks on organizations (Bakarich & Baranek, 2019), as cybersecurity incidents can materially affect financial statements, severely disrupt business operations, and damage organizational reputations (Boss *et al.*, 2022).

Boss *et al.* (2022) argue that cybersecurity awareness is crucial in the business world and essential for professionals who directly manage the impacts and costs of financial system breaches, particularly accountants. According to Allam *et al.* (2014), as risks and threats evolve and become more specialized, information security awareness plays a key role in mitigating the risk of security breaches.

Knowledge sharing, interventions, and collaborations enhance user awareness, which, in turn, shapes their attitudes and behaviors. Security breaches often result from users' lack of awareness, negligence, distraction, misconduct, apathy, or resistance (Safa *et al.*, 2015).

Nowadays, cyberattacks, cybercrimes, and cyber negligence are persistent concerns, highlighting the need to understand their impacts and material effects on financial statements, which justifies the inclusion of cybersecurity in accounting disciplines. In this context, Boss *et al.* (2022) developed case studies examining violations and their effects on financial reports, as well as tax, fiscal, managerial, and auditing consequences. One case specifically addresses the classification of costs related to cyber breaches into direct, indirect, and opportunity costs.

Lagazio *et al.* (2014) emphasize that classifying these costs is essential for understanding the total costs of cybercrime. Direct costs include expenses incurred in responding to a breach after detection, such as hiring forensic experts and law firms or providing identity protection services to affected individuals. Indirect costs involve expenses related to internal resources, including employees, time, and effort required to mitigate losses from a data breach. Opportunity costs stem from lost business opportunities due to reputational damage. Anderson *et al.* (2013) highlight that cost classification and measurement are challenging and subjective, requiring assessment both before the anticipated damage and after security measures are implemented. Awareness of these costs remains crucial in today's business environment.

Costs arise from deliberate cybersecurity breaches carried out by various actors. Hackers, for instance, employ a sophisticated range of methods to execute cyberattacks, targeting information confidentiality, integrity, and availability. Woo (2003) found that hackers are often driven by narcissistic tendencies, with a key characteristic being their desire to leave marks to gain admiration.

The risky behavior, authority, self-sufficiency, superiority, exhibitionism, exploitation, vanity, and sense of entitlement displayed by individuals with pronounced narcissistic traits can pose significant cybersecurity risks. Such individuals exhibit a sense of omnipotence, seeking to exploit others while believing they are entitled to special rights and privileges. They are intolerant of criticism, view themselves as self-sufficient, and display extreme vanity (Raskin & Terry, 1988). Narcissists engage in unethical behavior because their primary concern is with themselves (Curtis *et al.*, 2018).

Baumeister *et al.* (2000) argue that when people with narcissistic traits are challenged or contradicted, they tend to violate the source of the threat to protect their ego. Therefore, narcissists may feel encouraged to violate what they see as a source of threat. In this regard, Jones (2022) studies the psychology of cyber breaches and associates them with narcissism to find ways to minimize the effectiveness and damage caused by attacks.

A pervasive sense of superiority, grandiosity, entitlement, and dominance characterizes narcissism. Narcissists are highly self-centered, maintain an inflated self-view, and exhibit a negative correlation with empathy (Maasberg *et al.*, 2020). They often engage in malevolent behaviors driven by grandiosity, entitlement, and superiority rather than a deliberate intent to harm or negatively impact others. Their disregard for others stems from perceiving them as unimportant.

Avelino (2017) conducted a comprehensive study on narcissistic personality traits among undergraduate accounting students and found that higher levels of narcissism are associated with a greater tendency toward optimistic self-assessment. In this regard, such traits may also influence individuals' self-perception of their awareness of the costs associated with security breaches, both among students and professionals in the field.

Building on the previous discussion, this study addresses the following research question: **How do cybersecurity awareness and narcissistic personality traits influence the awareness of Brazilian accounting professionals and students concerning breach costs?** Specifically, it examines how cybersecurity awareness and narcissistic traits—such as self-sufficiency, overconfidence, and an inflated ego—affect the ability to recognize the challenges in assessing the cost impacts on financial statements, a complex and emerging issue.

The investigation of this relationship offers both theoretical and practical contributions. Theoretically, it expands the discussion on the studied themes, as prior research has examined breach costs and personality traits separately, leaving a gap in their integration. For instance, some studies have explored awareness of information security (Safa *et al.*, 2015) and the use of teaching cases on cyber awareness in business and accounting education (Bakarich & Baranek, 2019; Boss *et al.,* 2022; Cram & D'Arcy, 2016; Janvrin & Wang, 2022; Reidenbach & Wang, 2021; Roohani & Zheng, 2019). Other studies have analyzed accountants' roles in cybersecurity risk management, consulting, and protection (Eaton, Grenier, & Layman, 2019), assessed the economic and cost impacts of cyberattacks in the financial sector (Anderson *et al.*, 2013; Lagazio, Sherif, & Cushman, 2014; Silva, 2018), and examined the relationship between cyberattacks and dark personality traits (Curtis *et al.*, 2018; Jones, 2022; Jones *et al.*, 2021; Maasberg *et al.*, 2020).

Dark personality traits, such as narcissism, influence perceptions of self-sufficiency, vanity, and ego, potentially hindering students and professionals from recognizing the importance of cybersecurity in organizations. Previous studies have yet to examine this specific relationship though.

Regarding practical contributions, the empirical application involving accounting students and professionals enables the analysis of their perceptions, knowledge, challenges, and convictions about cybersecurity, highlighting the ongoing need for training and educational programs. Furthermore, this study is particularly relevant as it fosters reflection on the behavior of accounting students and professionals, including professors and entrepreneurs, who rely on technology and require secure and reliable information, communication, systems, and networks.

While implementing an information security system is costly for companies, the financial impact of a cyberattack is even more significant, particularly when compromised information leads to a loss of credibility and reputation. As Bakarich and Baranek (2019) highlight, the negative consequences of a cyberattack extend well beyond the immediate cost of the breach and may include reputational damage, increased protection expenses, litigation and legal risks, higher insurance premiums, and declines in stock prices and shareholder value.

2. Literature Review and Hypothesis Development

2.1 Cybersecurity

In Brazil, cybersecurity regulations are undergoing significant development. The federal government approved the National Cybersecurity Strategy (E-Ciber), enacted through Decree No. 10,222 on February 5, 2020, to establish national initiatives to strengthen cybersecurity measures.

CVM Resolution No. 35, issued on May 26, 2021, also provides recommendations for adopting a cybersecurity program to identify and assess internal and external cyber risks, reduce institutional vulnerability to cyberattacks, and implement internal procedures and controls—particularly in processing and managing customer data. The resolution emphasizes the need to "(...) develop and implement appropriate rules, procedures, and internal controls to ensure the confidentiality, authenticity, integrity, and availability of sensitive data and information" (p. 14, free translation).

Similarly, the General Data Protection Law (Law No. 13,709 of 2018) establishes guidelines for safeguarding fundamental rights to freedom and privacy in processing personal data, including in digital environments. Phishing attacks, large-scale denial-of-service incidents, data leaks involving private or institutional information, cyber espionage, and service disruptions are among the leading system breaches. They may be classified as infractions under this law.

2.2 Cybersecurity breaches and related costs

Cybersecurity breaches have accounting implications, including those outlined by Boss *et al.* (2022) concerning the financial impact of cyberattacks. Lagazio *et al.* (2014) categorize these direct, indirect, and opportunity costs.

Gordon and Loeb (2006) define direct costs as expenses resulting from specific security breaches. Boss *et al.* (2022) classify direct costs as those incurred in responding to a breach after its detection, including expenses related to hiring forensic experts and law firms and providing identity protection services to affected individuals.

Indirect costs, in contrast, while directly linked to security breaches, are broader in nature. They include expenses related to preventive measures, such as implementing security protocols and training employees to adopt cybersecurity best practices (Núcleo de Informação e Coordenação do Ponto BR, 2020). Boss *et al.* (2022) define indirect costs as those associated with internal resources, including employee time, effort, and other expenditures necessary to mitigate losses resulting from a data breach.

Finally, opportunity costs refer to expenses from lost business opportunities due to adverse reputational effects. These include revenue losses from increased customer churn, reduced income from system downtime, and higher costs of acquiring new business due to a damaged reputation (Boss *et al.*, 2022).

Boss *et al.* (2022) developed a teaching case focusing on the classification of cybersecurity breach costs. Similarly, Roohani and Zheng (2019) created ten teaching modules accompanied by professional videos to enhance cybersecurity education among students. In the same line of research, Reidenbach and Wang (2021) presented a case study for accounting students on the 2008 operational data breach at Heartland Payment, aiming to analyze the immediate accounting impacts, long-term operational consequences, and the company's sustainability.

Cram and D'Arcy (2016) proposed incorporating a foundational Information Security course to integrate essential technical knowledge with the managerial competencies required for business professionals. Similarly, Bakarich and Baranek (2019) developed a teaching case based on a real-world incident involving a U.S. public company that fell victim to a Business Email Compromise (BEC) scheme.

Anderson *et al.* (2013) systematically studied the costs associated with cybercrime, categorizing what is known and unknown about direct, indirect, and defense/protection costs in the United Kingdom and globally. The authors highlighted that indirect and transitory costs tend to be more burdensome, mainly because "cybercrimes are global and have strong externalities."

Lagazio *et al.* (2014) developed a multilevel model to examine the impact of cybercrimes on the financial sector. Their findings suggest that complex interactions between tangible and intangible factors influence the cost of cybercrimes, manifesting across various levels of society and the value network.

Silva (2018) analyzed the impacts of cyberattacks on Brazil's financial sector and developed a calculation methodology to assess the associated costs. Janvrin and Wang (2022) proposed an accounting framework for measuring cybersecurity, aiming to identify threats, risks, security events, and their implications while developing response strategies. Eaton *et al.* (2019) examined the role of accountants in cybersecurity risk management, discussing how their skills and competencies can add value at each of the five stages of the proposed model.

All these studies highlight the challenges and subjectivity in classifying and measuring costs. Anderson *et al.* (2013) argue that assessing the costs or benefits of security measures requires evaluating expenses both before the anticipated damage and after implementing security measures. Therefore, cybersecurity awareness is essential.

2.3 Cybersecurity awareness

Shaw *et al.* (2009) define cybersecurity awareness as "the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information control to protect the organization's data and networks" (p. 92). This understanding fosters awareness of the need to secure information, which, according to Landwehr (2001), involves three key areas: protecting received, stored, and retransmitted data; ensuring the integrity of processes executed on such data; and safeguarding the system's physical assets, such as backups, laptops, and printouts.

Safa *et al.* (2015) found that security awareness, organizational information security policies, experience and involvement in information security, attitudes toward information security, subjective norms, threat assessment, and information security self-efficacy positively influence user behavior.

Integrating procedures and technical controls is crucial for mitigating the risk of data breaches. When users disregard security procedures or policies and fail to embed them into the organizational culture, the environment becomes vulnerable to attacks and incurs breach-related costs (Albrechtsen & Hovden, 2010; Safa *et al.*, 2015). Based on this, **Hypothesis 1** is proposed: Cybersecurity awareness impacts awareness of breach costs.

Allam *et al.* (2014) emphasize that information security awareness is crucial in mitigating the risk of security breaches. By enhancing user awareness, it influences individuals' attitudes and behaviors. User behavior is a critical factor in this context, as negligence, ignorance, lack of awareness, mischief, apathy, and resistance are often key contributors to security breaches (Safa *et al.*, 2015). Based on these arguments, the hypothesis is further divided into: H1a: Cybersecurity awareness negatively impacts the difficulty in classifying breach costs; H1b: Cybersecurity awareness positively impacts convictions about accurately classifying breach costs; H1c: Cybersecurity awareness positively impacts knowledge about the impacts of breach costs on financial statements.

2.4 Cybersecurity and Narcissistic Personality Traits

Several studies (e.g., Curtis *et al.*, 2018; Maasberg *et al.*, 2020; Jones *et al.*, 2021) have examined the impact of personality traits on cybersecurity breaches. These studies do not specifically address the core focus of this research though, which concerns the costs associated with security breaches.

Curtis *et al.* (2018) examined the relationship between three personality traits—Machiavellianism, narcissism, and psychopathy—and phishing effort, attack success, and end-user susceptibility to phishing emails. Their findings revealed that while all three traits were linked to individuals' efforts in crafting phishing emails, they did not predict phishing success. Users with high scores on these traits were more likely to perceive phishing emails as successful though. Notably, end-user narcissism was associated with greater vulnerability to receiving phishing emails.

Maasberg *et al.* (2020) examined the relationship between narcissistic, Machiavellian, and psychopathic traits and individuals' intentions to engage in cyber threats. Similarly, Jones *et al.* (2021) conducted two studies to investigate how individuals with these personality traits respond to cybercrime, finding a significant association between narcissists and psychopaths and their involvement in short-term cyberattacks.

Narcissism is particularly relevant as a pervasive sense of superiority, grandiosity, entitlement, and dominance characterizes it. Narcissists are highly self-centered, maintain an inflated self-view, and exhibit a negative correlation with empathy (Maasberg *et al.*, 2020). They may engage in malevolent behaviors driven by their sense of grandiosity, entitlement, and superiority rather than an explicit intent to harm or negatively impact others. Their disregard for others stems from perceiving them as unimportant.

For Campbell *et al.* (2011), the narcissistic personality trait comprises three components: the Self, interpersonal relationships, and self-regulatory strategies. The narcissistic Self is marked by positivity, a sense of specialness and uniqueness, vanity, entitlement, and a strong desire for power and self-esteem.

Narcissistic relationships are characterized by low levels of empathy and emotional intimacy and are often superficial, ranging from engaging and exciting to manipulative and exploitative. Narcissistic strategies reinforce inflated self-views, leading individuals to seek attention and admiration, boast, take credit for others' achievements, and engage in risky relationship behaviors. In the specific context of accounting, Avelino and Lima (2017) found that students endorsed the unrestrained pursuit of pleasure, which could align with a propensity for cyber breaches.

Jones (2022) examined the personality traits of narcissism, Machiavellianism, and psychopathy to understand why individuals with high levels of these traits engage in cybercrime. Regarding narcissism, the author suggested that narcissists might carry out attacks due to their sense of authority, overconfidence, and grandiosity. Among other findings, the study indicated that presenting lighter versions of persuasive messages could help protect overconfident end users from phishing attacks. Building on this discussion, it is posited that the narcissists' authority, overconfidence, and grandiosity lead to **Hypothesis 2**: The narcissistic personality trait influences awareness of breach costs. Specifically, this hypothesis is further divided into H2a: Individuals with more pronounced narcissistic traits are more likely to report less difficulty in classifying breach costs; H2b: Individuals with more pronounced narcissistic traits are more likely to report greater conviction regarding the accuracy of classifying costs; and H2c: Individuals with more pronounced narcissistic traits are more likely to report knowledge of the impacts of breach costs on financial statements.

3. Methodological Procedures

3.1 Study design, data collection, and sample

This study employed a theoretical-empirical methodological approach within a descriptive research design. It adopted a quantitative approach to describe and analyze the phenomenon under investigation. A survey was used as the data collection strategy.

Data were collected remotely through a questionnaire distributed via a Microsoft Teams Office Form link. The survey was emailed to accounting students enrolled in the 4th to 8th semesters at universities across Brazil and to accounting professionals, including professors, who attended a scientific conference on accounting in 2022. The universities comprised both public and private institutions from various Brazilian states. The scientific conference, the XX USP International Conference on Accounting, organized by the University of São Paulo (USP), is one of Brazil's most prominent accounting events.

The instrument was administered based on accessibility from October to December 2022, aiming to capture a significant and diverse sample of individuals who met the study criteria. The study was approved by the Institutional Review Board at the State University of Bahia (CAAE No. 65415822.0.0000.0057).

The form included a free and informed consent form, a questionnaire addressing demographic and social information, the Narcissistic Personality Inventory (NPI) (Raskin & Hall, 1979; Raskin & Terry, 1988), and questions addressing Cybersecurity Awareness and Breach Cost Awareness.

3.2 Research constructs and variables

In this study, the dependent construct is Awareness of Breach Costs. The instrument was based on a teaching/simulation case adapted by Boss *et al.* (2022), as shown in Table 1.

Table 1

Awareness of Breach Costs

Suppose you are the controller of a large company and become aware that the organization has suffered a cybersecurity breach affecting multiple servers during the current period. This breach exposed banking data and critical financial information of both the company and its customers. A cybersecurity firm has been hired to remediate the breach and implement preventive measures to avoid recurrence. You are responsible for assessing the financial impact of the breach though. Based on this context, you are tasked with classifying specific breach-related costs into direct costs (DC), indirect costs (IC), or opportunity costs (OC), as outlined below::			
Breach Costs	**CD**	**CI**	**OC**
- Forensic and investigative activities related to the breach			
- Employee awareness training			
- New security controls installed, including a new firewall and intrusion detection software			
- Regulatory fines related to the cybersecurity breach			
- Compensation to affected parties			
- Communications regarding the occurrence, status, and effect of the breach			
- Legal costs			
- Loss of revenue due to system downtime			
- Loss of business due to negative reputational effects			
- Reduced profits due to loss of reputation			
We would like to have your feedback on the classifications above:			
Did you have difficulty classifying these costs? ( ) Yes ( ) No			
If you were to assign a score from 0 to 5, how difficult was it? _____			
Are you completely convinced/confident that you got more than 70% of the classifications right, without any type of consultation? ( ) Yes ( ) No			
If you were to assign a score from 0 to 5, how confident are you? _____			
Suppose that one year after the initial cybersecurity breach, you learn that the company will face legal action related to the breach. Would you be able to report the impacts of the breach costs on the financial statements? ( ) Yes ( ) No			
If you were to assign a score from 0 to 5, how difficult was it? _____			
Do you consider it important to include knowledge about cybersecurity in the Accounting program curriculum for professional qualification? ( ) Yes ( ) No			

Source: Based on Boss et al. (2022)

From the application of this teaching/simulation case, three variables were defined within the construct "Awareness of Breach Costs," each being binary and qualitative: Difficulty in Classifying Costs (DCC) (1 – Yes, 0 – No); Conviction of Correctness regarding Cost Classifications (CACC) (1 – Yes, 0 – No); and Knowledge to Report the Impacts of Breach Costs on Financial Statements (CICVDC) (1 – Yes, 0 – No).

Cybersecurity Awareness (CyberSegCons) is an independent construct measured through nine statements rated on a 5-point Likert scale. A factor analysis was conducted to identify and define the underlying factors. The instrument included nine statements adapted from Safa *et al.* (2015) and Boss *et al.* (2022).

Table 2

Cyber Security Awareness

1- I am aware of a potential security threat.
2- I understand the risk of cybersecurity incidents from cybersecurity breaches.
3- I keep myself up to date in terms of information security awareness.
4- I have sufficient knowledge about the cost of cybersecurity breaches.
5- I share information security knowledge to increase my awareness.
6- I have a conceptual/theoretical understanding of cybersecurity.
7- I am knowledgeable about information security's managerial and organizational aspects and how they relate to general accounting topics.
8- I am knowledgeable about the procedures and internal controls adopted to perform continuous monitoring in situations of cyberattacks.
9- I am knowledgeable about cybersecurity's ethical and legal aspects and the accountant's responsibility in each of these areas.

Source: Based on Safa et al. (2015) and Boss et al. (2022)

There is also the independent construct Degree of Difficulty in Reporting the Impacts of Breach Costs on Financial Statements (GDICBC), aligned with the study by Boss *et al.* (2022).

Finally, the other independent construct, the Presence of Narcissistic Personality Traits (PontosNARC), consists of a single variable related to narcissistic personality traits. The Narcissistic Personality Inventory (NPI), comprising 40 statements, was adopted. According to Paulhus and Jones (2015), this instrument is the most effective in capturing the characteristics of grandiosity, self-sufficiency, and an inflated ego associated with subclinical narcissism. The NPI was nationally validated by Magalhães and Koller (1994) and applied by Avelino (2017) in accounting research.

Raskin and Hall (1979) and Raskin and Terry (1988) developed the Narcissistic Personality Inventory (NPI) to assess narcissistic personality traits. Its statements address factors such as authority, self-sufficiency, superiority, exhibitionism, exploitation, vanity, and a sense of entitlement. The NPI is a forced-choice measure, presenting pairs of statements that reflect narcissistic and non-narcissistic characteristics, where a score of 1 is assigned to narcissistic responses and 0 to non-narcissistic responses. The 40 statements are binary, and the total score is obtained by summing the points, with a maximum possible score of 40, generating a quantitative variable.

Gender, age, semester, and whether the participant had a paid activity were included as variables for students. The form intended for the professionals also collected information on their area of practice, length of experience, and educational background. These variables were incorporated as control variables in the model, as they are considered to potentially influence individuals' interpretations and decision-making processes, as suggested by Hambrick and Mason (1984). The authors argue that socioeconomic characteristics such as age, education, occupation, functional experience, and financial status are complex factors that contribute to a psychological understanding of human behavior. Hambrick (2007, p. 334) further emphasizes that "[…] executives' experiences, values, and personalities greatly influence their interpretations of the situations they face and, in turn, affect their choices."

It is important to note that the reliability coefficient of the investigated model, measured by Cronbach's Alpha, was 0.710 for all variables combined. This result indicates the internal consistency of the model under study.

3.3 Statistical Analysis

Regarding the statistical analysis, the study employed Descriptive Statistics (frequencies, means, standard deviation, maximum and minimum values), Factor Analysis, and Logistic Regression.

Descriptive statistics were used to summarize, describe, and interpret data from the study sample. Factor analysis was applied to simplify the Cybersecurity Awareness variables, as the instrument was adapted from the original study and did not fully replicate the baseline model. Finally, logistic regression was employed to examine the relationships between the dependent and independent variables, providing evidence of the probability of an event occurring. This technique was also appropriate for testing the research hypotheses. The study hypotheses were operationalized through logistic regression and structured according to the three variables of the dependent construct "Breach Cost Awareness."

This study employed specific equations to estimate the logistic regression model for students and professionals. The responses from the samples were categorized into three binary dependent variables: DCC—With or Without Difficulty in Classifying Costs; CACC—With or Without Conviction of Correctness regarding Cost Classifications; and CICVDC—With or Without Knowledge to Report the Impacts of Breach Costs on Financial Statements.

The following independent variables were included: Cybersecurity Awareness (CSC), Presence of Narcissistic Personality Traits (NARC), and Degree of Difficulty in Reporting the Impacts of Breach Costs on Financial Statements (GDICBC).

In addition to the independent variables, the following control variables were included for students: gender, age group, semester, and paid activity. These variables were selected based on studies by Allen, Fuller, and Luckett (1998) and Avelino (2017). The following section presents the three equation models related to students in this study.

$$DCC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 SEM_i + \beta_7 REM_i + \varepsilon_i$$

$$CACC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 SEM_i + \beta_7 REM_i + \varepsilon_i$$

$$CICVDC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 SEM_i + \beta_7 REM_i + \varepsilon_i$$

The control variables for professionals included gender, age group, activity, length of experience, and education. These variables were based on previous studies, such as Campbell et al. (2011) and Avelino (2017). The following section presents the three equation models of this study related to professionals.

$$DCC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 ATUA_i + \beta_7 EXP_i + \beta_7 FORM_i + \varepsilon_i$$

$$CACC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 ATUA_i + \beta_7 EXP_i + \beta_7 FORM_i + \varepsilon_i$$

$$CICVDC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 ATUA_i + \beta_7 EXP_i + \beta_7 FORM_i + \varepsilon_i$$

4. Results

Since data were collected from two groups—Accounting Science students and professionals working in the accounting field—the results are presented individually and descriptively and then discussed and compared, considering previous studies.

4.1 Study 1: Profile of Accounting Science students

Most students were women between 18 and 25 years, enrolled in the 6th to the 8th semester, employed in a paid job, and attending a public higher education institution in the Northeast region.

Table 3 shows that the maximum score for correct answers in cost classification was 80 points, with some participants scoring zero and an average score of 38.4. Regarding narcissistic traits, the sample had an average score of 11.79 out of a maximum of 40 points. The highest agreement was observed for the following statements: "I find it easy to manipulate people," "I like to take responsibility for making decisions," "I can convince people," "I will be a success," and "I see myself as a good leader."

Table 3
Descriptive statistics concerning the students' data

	N	Minimum	Maximum	Mean	Standard Deviation
Variáveis					
Narcissism Score	262	2	29	11,79	5,474
Total Correct Score Cost Ranking	262	0	80	38,40	18,144
N valid (from list)	262				

Source: Developed by the authors (2024).

These parameters confirm that the extracted factor effectively captures the variation in the original data, which was incorporated into the statistical model. Subsequently, logistic regression was applied (Table 4) due to the binary nature of the dependent variables. The Forward Wald method included significant variables and excluded non-significant ones. The chi-square test results indicated a joint significance of sig = .000 for the coefficients across the three models, suggesting that the variables included in the model accurately predict the investigated outcomes.

Table 4
Adjustment to the logistic regression model concerning the students' data students

	Stage	-2-log- Likelihood	Cox & Snell R^2	Nagelkerke R^2
DCC		196.129	,076	,136
CACC		215,930	,223	,338
CIVCDC	2	252,440	,253	,353

Note 1: Difficult to Classify Costs (DCC); Conviction of Correctness in Cost Classifications (CACC), Knowledge to Report the Impacts of Breach Costs on Financial Statements (CIVCDC).

Source: Developed by the authors (2024).

The model was considered adequate, with -2LL values below 1 for all three models. Based on the Cox & Snell test, 7.6%, 22.3%, and 25.3% of the variations in the log odds ratio of occurrence probability are explained by the independent variables DCC, CACC, and CICVDC, respectively. The statistical model accounts for 13.6%, 33.8%, and 35.3% of the variations observed in DCC, CACC, and CICVDC, respectively. Table 5 presents the coefficients, signs, and Wald test results, displaying only the variables included through the application of the Forward Wald method.

Table 5
Coefficients, Signs, and Wald test for students' data

	Variables	Expected sign	Observed Sign	Coefficient (B)	Exp(β)	Wald Test
						P-Value
DCC Model 1	Gender		-	1,056	,348	,004
	GDICVDC		+	,507	1,660	,001
	Constant		+	,559	1,749	,320
CACC Model 2	CSC	+	+	,668	1,950	,001
	GDICVDC		-	,800	,449	,000
	Gender		+	1,070	2,915	,002
	Semester		-	,552	,576	,001
	Constant		+	4,651	104,705	,000
CIVCDC Model 3	CSC	+	+	,929	2,531	,000
	GDICVDC		-	,839	,432	,000
	Constant		+	1,933	6,911	000

Note 1: Difficulty in Classifying Costs (DCC), Conviction of Accuracy in Cost Classifications (CACC), Knowledge to Report the Impacts of Breach Costs on Financial Statements (CIVCDC), Degree of Difficulty in Reporting the Impacts of Breach Costs on Financial Statements (GDICVDC), Cybersecurity Awareness (CSC).

Source: developed by the authors (2024)

The individual analysis of the parameters using Model 1 in Table 5 shows that the GDICVDC variable has a positive sign, indicating that increases in this variable are associated with a higher probability of students experiencing difficulty in classifying costs. In contrast, the Gender variable has a negative sign, suggesting that difficulty in classifying costs decreases as a function of this variable.

In Model 2, CyberSegCons and Gender have positive signs, indicating that conviction about correct answers increases with greater cybersecurity awareness and as a function of Gender. Conversely, conviction about correct answers decreases as a function of the semester the student is currently attending and GDICVDC.

In Model 3, the CSC sign was positive, indicating a probability that knowledge to report the impacts of breach costs on financial statements increases as a function of awareness about cybersecurity and decreases as a function of GDICVDC.

These findings demonstrate that, for students, greater cybersecurity awareness positively impacts awareness of breach costs. The only relationship not observed concerns difficulty classifying costs, which may be attributed to the students' level of education. This result aligns with Anderson *et al.* (2013), who argue that identifying breach costs requires cybersecurity awareness. Regarding narcissistic traits, no statistical significance was found, contradicting the expectation that individuals with a self-view of superiority and grandiosity, as highlighted by Maasberg *et al.* (2020), would exhibit greater awareness.

4.2 Study 2: Profile of Professionals in the Accounting Area

Most professionals were male, between 26 and 35 years old, had completed higher education, and worked in a public or private company in the Southeast region. Table 6 shows that the maximum score for correct answers in cost classification was 80 points, with some participants scoring zero and an average score of 44.7. Regarding narcissistic traits, the sample had an average score of 12.76, with the highest agreement for the following statements: "Modesty does not become me," "I like to take responsibility for making decisions," "I am a confident person," "I see myself as a good leader," and "I have a natural talent for influencing people."

Table 6
Descriptive statistics concerning the professionals' data

	N	Minimum	Maximum	Mean	Standard Deviation
Professionals					
Narcissism Score	166	2	32	12,76	6,559
Total Correct Score Cost Ranking	166	0	80	44,70	19,530
N valid (from list)	166				

Source: developed by the authors (2024).

Next, factor analysis was conducted to group the items related to Cybersecurity Awareness, resulting in the extraction of the Cybersecurity Awareness (CSC) factor. For students, the Bartlett test indicated that the model was statistically significant (sig. < 0.00), while the KMO value, which measures the adequacy of the data for factor analysis, was 86.8%. The eigenvalue was 4.592, accounting for 51.026% of the explained variance. For professionals, the Bartlett test also showed statistical significance (sig. < 0.00), with a KMO value of 0.717. The eigenvalue was 3.822, explaining 42.467% of the variance.

Finally, logistic regression was applied using the Forward Wald method (Table 7).

Table 7
Adjustment to the logistic regression model concerning the professionals' data

	Stage	-2-log- Likelihood	Cox & Snell R^2	Nagelkerke R^2
DCC	3	169.222	,128	,187
CACC	2	153,796	,084	,132
CICVDC	4	136,539	,376	,518

Source: developed by the authors (2024).

Table 8

Coefficients, Signs, and Wald test for professionals' data

	Variables	Expected Sign	Observed Sign	Coefficient (B)	Exp(β)	Teste de Wald
						P-Value
DCC Model 1	CSC	-	-	,430	,651	,038
	GDICVDC		+	,299	1,348	,027
	Gender		-	1,176	,308	,008
	Constant		+	,898	2,455	,139
CACC Model 2	CSC	+	+	,699	2,012	,002
	TempoExp		+	,248	1,282	,027
	Constant		-	2,250	,105	,000
CICVDC Model 3	NARC	+	+	,118	1,125	,001
	CSC	+	+	1,103	3,012	,000
	GDICVDC		-	1,110	,329	,000
	Education		+	2,319	10,169	,003
	Constant		-	3,322	,036	,041

Note 1: Difficulty in Classifying Costs (DCC), Conviction of Accuracy in Cost Classifications (CACC), Knowledge to Report the Impacts of Breach Costs on Financial Statements (CIVCDC), Degree of Difficulty in Reporting the Impacts of Breach Costs on Financial Statements (GDICVDC), Cybersecurity Awareness (CSC), , Narcissistic Traits Score (NARC).

Source: developed by the authors (2024).

The individual analysis of the parameters using Model 1 in Table 8 shows that the CSC variable has a negative sign, indicating that a decrease in cybersecurity awareness is associated with a higher probability of professionals experiencing difficulty in classifying costs. In contrast, the GDICVDC variable has a positive sign, suggesting that increased difficulty in reporting breach cost impacts is linked to greater difficulty in classifying costs.

In Model 2, CSC and time of experience had a positive sign, suggesting that conviction about correct classifications increases with greater cybersecurity awareness and professional experience.

In Model 3, Narcissism, CSC, and Education showed positive signs, suggesting that knowledge of the impacts of breach costs on financial statements is likely to increase as a function of these variables and decrease as a function of GDICVDC.

These findings demonstrate that, for professionals, greater cybersecurity awareness directly impacts awareness of breach costs, reinforcing what Anderson *et al.* (2013) argue that cybersecurity awareness is essential for identifying breach costs. Regarding narcissistic traits, the results generally did not show statistical significance, once again contradicting the expectation highlighted by Maasberg *et al.* (2020) that individuals with a self-view of superiority and grandiosity would exhibit greater awareness. Unlike students, however, professionals with more pronounced narcissistic traits demonstrated greater knowledge of the impacts of breach costs on financial statements than those with fewer traits.

5. Discussion

To initiate the discussion, Table 9 presents the decisions regarding the research hypotheses formulated in this study.

Table 9
Decision on the Research hypotheses

Hypotheses	Dependent Variable	Independent Variable	Decision	
			Students	Professional
Hypothesis 1: Cybersecurity awareness impacts awareness of breach costs.			**Partially rejected**	**Failed to be rejected**
H1a: Cybersecurity awareness negatively impacts the difficulty in classifying breach costs	DCC	CSC	Rejected	Failed to be rejected
H1b: Cybersecurity awareness positively impacts convictions about accurately classifying breach costs	CACC	CSC	Failed to be rejected	Failed to be rejected
H1c: Cybersecurity awareness positively impacts knowledge about the impacts of breach costs on financial statements	CIVCDC	CSC	Failed to be rejected	Failed to be rejected
Hypothesis 2: The narcissistic personality trait influences awareness of breach costs			**Rejected**	**Partially rejected**
H2a: Individuals with more pronounced narcissistic traits are more likely to report less difficulty in classifying breach costs.	DCC	NARC	Rejected	Rejected
H2b: Individuals with more pronounced narcissistic traits are more likely to report greater conviction regarding the accuracy of classifying costs.	CACC	NARC	Rejected	Rejected
H2c: Individuals with more pronounced narcissistic traits are more likely to report knowledge of the impacts of breach costs on financial statements.	CIVCDC	NARC	Rejected	Failed to be rejected

Source: Developed by the authors (2024).

The results of this study warrant attention from the accounting field. Both students and professionals in the sample exhibited difficulty in classifying breach costs, uncertainty in reporting these costs in financial statements, and a lack of conviction regarding the correct classification of costs. Although professionals performed better than students in classifying breach costs, the average score remained below 50 out of a possible 100. The broader lack of cybersecurity awareness, qualification, and knowledge among many Brazilians engaged in the digital world suggests that Brazilian society is not yet adequately prepared to use digital tools with the necessary cybersecurity precautions (Decree No. 10,222, 2020).

These findings also support the argument by Boss et al. (2022) that cyber awareness is a critical topic that, in the practical context of accounting, contributes to the development of better-informed professionals. From this perspective, they assert that cybersecurity should not be treated as an "add-on" or an additional subject in accounting but as an integral component of the field. Interestingly, despite growing regulatory and professional emphasis, most accounting curricula still confine cybersecurity coverage to the Accounting Information Systems discipline.

When analyzing the tendency toward narcissistic traits, professionals exhibited a stronger inclination, confirming their lack of modesty and greater confidence in their decisions. Among students with more pronounced narcissistic traits, a notable finding was their agreement with the ease of manipulating people. Both groups reported seeing themselves as good leaders and enjoying taking responsibility for their decisions though. This suggests that self-sufficiency, vanity, and an inflated ego were present among the respondents, which may indicate a lack of preparedness to handle today's increasingly complex and persistent cyber threats. This result is partially supported by Avelino and Lima (2017), who found that Accounting Science students more frequently identified themselves as good leaders.

When analyzing the respondents' cybersecurity awareness, students and professionals with higher cybersecurity awareness exhibited greater conviction in classifying costs correctly and a better ability to report their impacts on financial statements. Additionally, professionals showed less difficulty in classifying costs and reporting their impacts on financial statements.

These findings align with those of Safa *et al.* (2015), which suggest that professionals with greater security awareness tend to exhibit more responsible user behavior. They also support the findings of Boss *et al.* (2022) regarding student perceptions, highlighting the subjectivity involved in cost classification and the challenges of measuring breach costs. Moreover, there was broad agreement on the importance of addressing these topics in accounting education, as reflected in this study's results, where 80.2% of respondents supported the inclusion of cybersecurity-related content in accounting curricula.

Additionally, these findings reinforce the arguments of Reidenbach and Wang (2021) regarding the importance of incorporating teaching cases into Accounting programs. Such cases allow students to engage with real-world scenarios, enabling them to develop and apply their skills while fostering critical thinking in evaluating decisions made by companies, external auditors, and shareholders.

Furthermore, the findings align with the argument of Boss *et al.* (2022) that introducing, emphasizing, and integrating cybersecurity topics into accounting curricula can benefit students and future professionals significantly. The authors do not suggest shifting the overall focus of accounting education but advocate for incorporating discussions—similar to those proposed by Roohani and Zheng (2019)—on supplementing the current curriculum. This approach aims to equip students with the necessary knowledge and skills to assess cybersecurity risks and understand the controls needed to mitigate them, particularly in light of recent and ongoing cybersecurity incidents.

Finally, regarding narcissistic traits, it is noteworthy that professionals with more pronounced narcissistic traits were more likely to report knowing the impacts of breaches on financial statements. Additionally, gender, length of experience, and education were significant factors in the professional sample, while gender and current semester stood out in the student sample. These findings support the assumption of Upper Echelons Theory (Hambrick & Mason, 1984; Carpenter *et al.*, 2004), which posits that social and demographic factors influence individuals' choices.

The absence of statistical significance regarding greater or lesser awareness of breach costs among individuals with more pronounced narcissistic traits suggests that, even if these respondents recognized their lack of knowledge on the subject, they would not acknowledge their limitations. This aligns with their tendency toward superiority, grandiosity, and an inflated perception of their abilities, as highlighted by Maasberg *et al.* (2020) and Raskin and Terry (1988).

6. Conclusion

Cyber breaches compromise the confidentiality and integrity of financial information within organizations. In many cases, attacks are facilitated by a lack of awareness regarding risks such as sharing account information, downloading software from unverified sources, writing down passwords on paper, and opening emails from unknown or suspicious senders (Safa *et al.*, 2015).

This study aimed to analyze the influence of narcissistic traits on cybersecurity awareness and breach cost awareness among accounting students and professionals. The results indicated that both groups struggled with classifying breach costs and reporting them in financial statements, as evidenced by the total number of correct answers in cost classification not exceeding 50 points.

According to the literature, cybersecurity awareness was expected to enhance students' and professionals' knowledge of reporting the impacts of breach costs on financial statements and their confidence in cost classification. The findings confirmed that individuals with greater cybersecurity awareness were more likely to report a stronger conviction in correctly classifying costs and recognizing their impacts on financial statements.

Regarding the narcissistic trait, professionals scored higher and demonstrated greater knowledge in reporting breach costs in financial statements. Narcissistic personality traits did not seem to influence the other results though.

Thus, these findings address the research problem, confirming that cybersecurity awareness influences awareness of breach costs among the accounting professionals and students surveyed. Additionally, the results indicate that the narcissistic personality trait does not significantly impact breach cost awareness as initially expected, except that narcissistic professionals demonstrated greater knowledge in reporting breach costs in financial statements.

The results contribute to the scientific field of Accounting, as they encourage a reflection on the influence of narcissistic personality traits on the behavior of students and professionals. Additionally, it allows for individualized and comparative analysis of perception, knowledge, difficulties, and convictions about cybersecurity and the impacts of breach costs on accounting statements.

This study also highlights the need for educational institutions to integrate cybersecurity concepts more effectively into the curricula of Accounting Sciences programs. Disciplines such as General Accounting, Management Accounting, Cost Accounting, Controllership, Financial Administration, Business Budgeting, Analysis of Accounting Statements, and Auditing should incorporate these topics to enhance students' ability to recognize the impacts of cyberattacks on financial statements. Additionally, promoting extracurricular activities focused on cybersecurity can further support teaching and learning in this emerging and critical field.

These findings also highlight the need for educators to prepare for this evolving landscape and to incorporate concrete case studies that allow students to engage with real-world cybersecurity breach scenarios, as demonstrated in this study. Additionally, they underscore the importance for business professionals to invest in the implementation of information security systems. Although such investments may be costly, their financial impact is likely to be significantly lower than that of a cyberattack—particularly when compromised information leads to reputational damage and a loss of credibility for companies.

These results are expected to encourage reflection among accounting education institutions and companies, promoting the introduction of more specialized training and cybersecurity content within Accounting disciplines. Integrating these topics with other curricular subjects will help aspiring accountants develop the ability to recognize the financial impacts of cyberattacks and the associated recovery costs for companies.

This study has limitations, particularly regarding the sample size and the behavioral—rather than clinical—analysis of narcissistic traits. Additionally, examining self-sufficient, vain, and self-centered behaviors, which tend to overlook personal weaknesses and the need to develop new skills and competencies for professional practice, presents another constraint.

Future studies are encouraged to expand the sample spectrum, apply new teaching cases inspired by international studies, and further explore the debate on integrating cybersecurity content and its impact on accounting records into the regulations governing national and international accounting education.

References

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: a victim of operational pressures. *Computers & Security, 42*, 56-65.

Allen, J., Fuller, D., & Luckett, M. (1998). Academic integrity: behaviors, rates and attitudes of business students toward cheating. *Journal of Marketing Education, 20*(1), 41-52.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M. J. van, Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In Böhme, R. (eds). *The Economics of Information Security and Privacy*. Springer, Berlin, Heidelberg. (pp. 265-300). https://doi.org/10.1007/978-3-642-39498-0_12

Avelino, B. C. (2017). Olhando-se no espelho: uma investigação sobre o narcisismo no ambiente acadêmico. [Tese de doutorado, Universidade de São Paulo]. Biblioteca Digital. https://doi.org/10.11606/T.12.2017.tde-06042017-165713

Avelino, B. C., & Lima, G. A. S. F. (2017). Narcisismo e desonestidade acadêmica. *Revista Universo Contábil, 13*(3), 70. doi:10.4270/ruc.2017319

Bakarich, K. M., & Baranek, D. (2019). Something phish-y is going on here: a teaching case on business email compromise. *Current Issues in Auditing, 14*(1), A1-A9.

Baumeister, R. F., Bushman, B. J., & Campbell, W. K. (2000). Self-esteem, narcissism, and aggression: does violence result from low self-esteem or from threatened egotism? *Current Directions in Psychological Science, 9*, 26-29.

Boss, S. R., Gray, J., & Janvrin, D. J. (2022). Accountants, cybersecurity isn't just for "techies": incorporating cybersecurity into the accounting curriculum. *Issues in Accounting Education, 37*(3), 73-89.

Campbell, W. K., Hoffman, B. J., Campbell, S. M., & Marchisio, G. (2011). Narcissism in organizational contexts. *Human Resource Management Review, 21*(4), 268-284.

Carpenter, M. A., Geletkanycz, M. A., & Sanders, G. M. (2004). Upper echelons research revisited: antecedents, elements and consequences of top management team composition. *Journal of Management*, *30*(6), 749-778.

Cram, W. A., & D'Arcy, J. (2016). Teaching information security in business schools: current practices and a proposed direction for the future. *Communications of the Association for Information Systems*, *39*(1), 3.

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: patterns of attack and vulnerability. *Computers in Human Behavior, 87*, 174-182.

Decreto n. 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13*(2), C1-C9.

Gordon, L. A., & Loeb, M. P. (2006). *Managing cybersecurity resources: a cost-benefit analysis* (Vol. 1). New York: McGraw-Hill.

Hambrick, D. C. (2007). Upper echelons theory: an update. *Academy of Management Review, 32*(2), 334-343.

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: the organization as a reflection of its top managers. *Academy of Management Review, 9*(2), 193-206.

Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: an event, impact, response framework. *Accounting Horizons, 36*(4), 67-112.

Jones D. N. (2022). Shadows behind the keyboard: dark personalities and deception in cyberattacks. *Proceedings of the 2022 ACM International Workshop on Security and Privacy Analytics (IWSPA '22)*, April 27, 2022, Baltimore, MD, USA. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3510548.3519379

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.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, *45*, 58-74.

Landwehr, C. E. (2001). Computer security. *International Journal of Information Security, 1*(1), 3-13.

Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Maasberg, M., Slyke, C. Van, Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM, 63*(12), 64-80.

Magalhães, M., & Koller, S. H. (1994). Relação entre narcisismo, gênero e gênero. *Arquivos Brasileiro de Psicologia, 46*(3/4), 77-93.

Núcleo de Informação e Coordenação do Ponto BR. (2020). *Segurança digital: uma análise da gestão de riscos em empresas brasileiras* [livro eletrônico]. Comitê Gestor da Internet no Brasil. https://www.nic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf

Paulhus, D. & Jones, D. (2015). *Measures of dark personalities*. In Boyle, G. J., Saklofske, D. H., & Matthews, G. (Eds.). *Measures of personality and social psychological constructs* (pp. 562-594). Elsevier. 10.1016/B978-0-12-386915-9.00020-6

Raskin, R., & Hall, C. S. (1979). A narcissistic personality inventory. *Psychological Reports*, *45*, 590.

Raskin, R., & Terry, H. (1988). A principal-components analysis of the narcissistic personality inventory and further evidence of its construct validity. *Journal of Personality and Social Psychology, 5*4(5), 890-902.

Reidenbach, M., & Wang, P. (2021). Heartland payment systems: cybersecurity impact on audits and financial statement contingencies. *Issues in Accounting Education*, *36*(2), 93-109.

Resolução CVM n. 35, de 26 de maio de 2021. Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários. https://conteudo.cvm.gov.br/legislacao/resolucoes/resol035.html

Roohani, S. J. & Zheng, X. (2019). Using ten teaching modules and recently publicized data-breach cases to integrate cybersecurity into upper-level accounting courses. In Calderon, T. G. (Ed.). *Advances in accounting education: teaching and curriculum innovations*. (Vol. 23), Emerald Publishing Limited, Bingley (pp. 113-125). https://doi.org/10.1108/S1085-462220190000023007

Safa, N. S., Sookhak, M., Solms, R. Von, Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Silva, W. R. (2018). *Análise econômica dos impactos de ataques cibernéticos*. [Dissertação de Mestrado, Faculdade de Economia, Administração e Contabilidade da Universidade de Brasília]. Repositório Aberto da Universidade de Brasília. http://repositorio.unb.br/handle/10482/34838

Woo, H-J. (2003). *The hacker mentality: exploring the relationship between psychological variables and hacking activities.* Dissertação [Doutorado em Filosofia, University of Georgia].

Annex 1 – Original extract from Boss *et al.* (2022), which was used as inspiration for defining the construct "Breach Cost Awareness"

1. Identify which of the following expenses are direct vs indirect vs lost opportunity costs.

Expense	Direct costs	Indirect costs	Lost opportunity costs
Forensic and investigative activities related to breach			
Penetration testing to ensure vulnerabilities addressed			
Costs associated with issuing new accounts / credit cards			
Employee awareness training			
Installed new security controls including a new firewall and intrusion detection software			
Added a new IT position, chief information security officer			
Regulatory fines related to cybersecurity breach			
Compensation to affected parties			
Communications regarding status and effect of breach			
Loss of customers			
Legal costs			
Public relations costs			
Credit monitoring costs			
Lost revenue from system downtime			
Lost business due to negative reputation effects			
Shortfall in profits due to loss of reputation			

2. Which of these costs are easiest to measure? Why?

3. Which of these costs are most difficult to measure? Why?

4. When could you measure (or estimate) each cost? Why?