

Invisible Threats, Visible Stress: Cybersecurity Anxiety as a Pathway Linking Cyber Threat Exposure to Student Mental Health

Daniel Opoku

dopoku@uew.edu.gh

University of Education

Samuel Oduro Owusu

Manipal Academy of Higher Education

Article

Keywords: Mental Health, Cyber threat, Cybersecurity, digital wellbeing, Digital Risk, Stress and coping theory

Posted Date: March 26th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-9066978/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License. [Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

The recent pace of digitalisation in the higher education sector has increased university students' vulnerability to cyber threats, thereby creating psychological risks that extend beyond technical and financial consequences. This study examines the mediating role of cybersecurity anxiety in the relationship between cyber threat exposure and mental health among university students. Drawing on Stress and Coping Theory and Technology Threat Avoidance Theory, the study employs a quantitative cross-sectional survey design and analyses data from 563 university students. The hypothesised relationships were tested using Structural equation modelling. The findings indicate that cyber threat exposure significantly predicts mental health outcomes and higher levels of cybersecurity anxiety. In addition, cybersecurity anxiety is significantly associated with mental health and partially mediates the relationship between cyber threat exposure and mental health. These results suggest that cyber threats function as psychosocial stressors that influence student well-being both directly and indirectly through anxiety-related psychological processes. The study contributes to digital well-being and cybersecurity literature by identifying cybersecurity anxiety as a key psychological mechanism linking cyber risk exposure to mental health outcomes. Practically, the findings highlight the need for higher education institutions to integrate cybersecurity education with student mental health support services. The study underscores the importance of addressing cybersecurity risks as part of holistic student wellbeing strategies in increasingly digital academic environments.

1. Introduction

The rapid adoption of digital technologies in the higher education sector has significantly increased students' susceptibility to online threats, including phishing, account compromise, malware, cyberbullying, and identity-related fraud. University students constitute a highly vulnerable group, as much of their activity involves online communication, data exchange, and constant use of the institutional information system for study and [1, 2]. Empirical studies across multiple contexts report a substantial prevalence of cyber-victimisation and related incidents among tertiary students, making cyber risk an important emerging stressor in the student experience [1]. Exposure to cyber threats produces not only technical and financial harms but also psychological consequences. Systematic and primary studies indicate elevated rates of anxiety, depressive symptoms, stress, and other adverse mental-health outcomes among students who experience cyber-victimisation or cyber incidents [2, 3]. For example, recent large-scale reviews and empirical papers document consistent associations between various forms of online victimisation and poorer mental-health indicators among university populations, suggesting that cyber incidents are a nontrivial contributor to student psychological morbidity [3]. Understanding the psychological pathway from cyber threat exposure to mental-health outcomes requires a theoretical lens that links environmental stressors to emotional responses. Stress and Coping Theory [4] provides a parsimonious framework: individuals appraise environmental demands (threats) and subsequently mount coping responses, with emotional reactions, notably anxiety, arising from threat appraisal and affecting downstream wellbeing. Within the cybersecurity domain, Technology Threat Avoidance Theory (TTAT) refines this logic by specifying threat appraisal and coping appraisal processes for information technology threats. TTAT highlights that when perceived avoidability is low, users may engage in emotion-focused coping, including heightened fear or anxiety, rather than problem-focused remediation [5]. These theoretical perspectives jointly explain why exposure to cyber threats may translate into cybersecurity-specific anxiety and, ultimately, into broader mental health consequences [6]. Despite the plausibility of this pathway, empirical research testing cybersecurity anxiety as a mediating mechanism between cyber threat exposure and general mental health among university students remains limited. Existing studies have predominantly documented bivariate associations or examined behavioural responses to cyber threats (e.g., protective behaviours) but have seldom tested process models that position technology-specific anxiety as the proximal psychological mechanism linking exposure to mental-health outcomes [1, 3]. This evidence gap constrains theoretical development and limits actionable insights for university mental-health and cybersecurity interventions, both of which would benefit from knowing whether reducing anxiety (for example, through psychoeducation or resilience training) could attenuate the mental-health impact of cyber incidents. Accordingly, the present study investigates whether cybersecurity anxiety mediates the relationship between cyber threat exposure and mental health among university students. Grounded in Stress and Coping Theory and contextualised by TTAT, the study tests a mediation model in which cyber threat exposure predicts heightened cybersecurity anxiety, which in turn predicts poorer mental-health indicators (e.g., anxiety, depressive symptoms, psychological distress). Establishing this mediating pathway will (a) advance theory by clarifying the emotional process that connects cyber incidents to psychological outcomes, and (b) inform university policy and practice by identifying a proximal target (cybersecurity anxiety) for interventions aiming to protect student mental health.

2 Literature Review

Drawing on the Stress and Coping Theory and the Technology Threat Avoidance Theory, the review provides a conceptual basis for explaining how environmental stressors, namely cyber threats, might trigger an affective reaction that, in turn, determines the impact on psychological well-being. It begins by presenting the study's theoretical framework, then presents a systematic review of the empirical literature addressing the direct relationships among exposure to cyber threats, cybersecurity anxiety, and mental health, and finally considers how cybersecurity anxiety mediates these relationships. The review concludes with a description of the conceptual framework within which the subsequent investigation will be conducted.

2.1 Theoretical Framework

This study is underpinned by Stress and Coping Theory [4], with Technology Threat Avoidance Theory (TTAT) [5] providing contextual support in the cybersecurity domain. Stress and Coping Theory holds that psychological outcomes stem from individuals' cognitive appraisals of environmental stressors and their perceived ability to cope with them. When an ecological demand is appraised as threatening and coping resources are perceived as inadequate, negative emotional responses, particularly anxiety, are elicited, which may subsequently impair mental health. In the present study, cyber threat exposure is an environmental stressor, cybersecurity anxiety is the emotional response to threat appraisal, and mental health is the psychological outcome of sustained exposure and anxiety. Technology Threat Avoidance Theory extends this logic by focusing specifically on information-technology threats. TTAT explains how perceived severity and susceptibility to technology-related threats elicit fear and anxiety responses, particularly when users perceive threats as complex to avoid or control [5]. In a university context, repeated exposure to cyber threats such as phishing, account compromise, and data breaches may heighten

students' perceived vulnerability, thereby increasing cybersecurity anxiety and negatively affecting mental health. Together, these theories provide a coherent framework for understanding how cyber threat exposure translates into adverse mental-health outcomes through cybersecurity anxiety.

2.2 Cyber Threat Exposure and Mental Health

Cyber threat exposure refers to individuals' direct or indirect experiences of harmful online behaviours, including cyberbullying, phishing, identity theft, online fraud, and unauthorised access to online accounts. For university students, the common use of digital platforms for studying, paying bills, and socialising increases the likelihood of being compromised by such threats and the perceived severity of these threats [1]. This connection may be explained by Stress and Coping Theory. According to this theory, a person's mental health is determined by how they appraise the stressors around them and the extent to which they believe they can handle them [4]. Being a victim of cyber threats in a university environment is an uncontrollable and usually unpredictable stressor. Negative reactions manifest when students perceive cyber threats as real and believe they lack adequate resources to deal with them, including cybersecurity knowledge or institutional support. Such sentiments may accumulate over time and develop into more significant mental health issues. A great number of studies repeatedly demonstrate that cyber threat exposure is strongly linked to adverse mental health outcomes [2]. According to recent research, students subjected to cyber-victimisation are more anxious, depressed, stressed, and generally in psychological distress compared to those who are not subjected to such experiences [2]. Wang et al. [7] examined the effects of exposure to online risks on anxiety among college students and the mediating role of cognitive and interpersonal factors. The systematic review by Arif et al. [3] also shows that exposure to cyberbullying and other online threats is associated with poorer mental health among university students across numerous environments. In terms of stress, continuous exposure to cyber threats is a chronic stressor that may result in deterioration of psychological health over time. Building on this theoretical and empirical evidence, the next hypothesis is put forward:

H1: Cyber threat exposure is significantly associated with mental health among university students.

2.3 Cyber Threat Exposure and Cybersecurity Anxiety

Exposure to cyber threats has been extensively identified as a profound antecedent of cybersecurity anxiety, particularly among groups with high digital engagement, such as university students. Cyber threat exposure refers to individuals' experiences of malicious online activities, including phishing attacks, malware attacks, unauthorised account access, and online fraud. For university students, constant exposure to academic and social digital media increases the likelihood of encountering cyber threats and heightens the psychological salience of such exposure [8, 9]. In theory, the Stress and Coping Theory explains the development of anxiety in response to cyber threat exposure through cognitive appraisal mechanisms. According to Lazarus and Folkman [4], anxiety arises when people evaluate environmental demands as threatening and believe they have insufficient resources to deal with them. Cyber threats are often unpredictable, technically complex, and perceived as difficult to control, making them particularly likely to be perceived as threatening. Such risks lead to increased worry, fear, and vigilance regarding digital safety, thereby raising cybersecurity anxiety over time. Technology Threat Avoidance Theory (TTAT) also helps contextualise this association, as it focuses on technology-specific threat perception. TTAT holds that beliefs about severity and vulnerability to information-technology threats cause fear and anxiety, especially when individuals perceive avoidance or mitigation measures to be ineffective [4]. The dependence of the university student population on common networks, individual devices, and institutional systems may heighten perceived vulnerability, thereby increasing anxiety reactions to exposure to cyber threats. This theoretical connection is supported by empirical data. Research has found that when people report increased exposure to cyber threats, they report high levels of technology-related fear and anxiety [10]. Shillair et al. [9] found that exposure to online security threats was positively correlated with cybersecurity anxiety, particularly among users with low perceived control and cybersecurity confidence. These results suggest that exposure to cyber threats is a direct psychological inducer of cybersecurity anxiety, rather than a background risk factor [11]. Exposure to cyber threats can be particularly anxiety-inducing in the university setting, as cyber incidents can interrupt academic progress, disrupt financial security, and damage social image. Students may experience lingering anxiety when using critical internet solutions due to concerns about compromised academic accounts, identity theft, or internet fraud. In general, the theoretical and empirical evidence supports a positive and significant correlation between cyber threat exposure and cybersecurity anxiety among university students. Based on the discussion above, the hypothesis to be put forward is the following:

H2: Cyber threat exposure is significantly associated with cybersecurity anxiety among university students.

2.4 Cybersecurity Anxiety and Mental Health

Cybersecurity anxiety refers to a sustained state of anxiety, fear, and emotional unease regarding perceived risks to online security, privacy, and personal information. Although this anxiety may be context-dependent, it shares core psychological features with general anxiety, including attenuation, rumination, and affective strain. Stress and Coping Theory holds that chronic anxiety arising from unresolved or repeated stressors has adverse health consequences for the mind [4]. Empirical research on technology-related anxieties shows a strong association with poorer mental health [12]. Studies indicate that individuals who express greater concern about online security experience higher levels of psychological distress, anxiety symptoms, and reduced well-being [11]. Cybersecurity anxiety can result in persistent fear of data breaches, identity theft, or financial loss, which further heightens stress reactions and contributes to broader mental health challenges. The psychological effects of cybersecurity anxiety may be particularly intense among university students. Academic work, communication, and financial transactions rely heavily on digital platforms, making digital security issues both highly relevant and ongoing. Empirical studies of student groups indicate that anxiety over online safety is linked to increased emotional distress and depressive symptoms, particularly when students feel they lack adequate control over the cybersecurity threat [8, 12]. Persistent anxiety over cybersecurity can also exacerbate other academic stressors, increasing susceptibility to mental health problems. Theoretically, Technology Threat Avoidance Theory supports this relationship, as fear and anxiety are proximal psychological consequences of perceived technology threats, which include behavioural reactions and influence on overall psychological well-being [5]. The development of mental health problems is prevented from worsening only if anxiety remains acute and coping capacity and emotional regulation remain effective. The literature supports an important connection between cybersecurity anxiety and mental health, with higher levels of cybersecurity anxiety associated with worse mental health outcomes [13]. This relationship confirms the importance of investigating cybersecurity anxiety

as a relevant psychological variable determining the well-being of students in digitally intensive educational settings. On the basis of this evidence, the following hypothesis is suggested:

H3: Cybersecurity anxiety is significantly associated with mental health among university students.

2.5 Mediating Role of Cybersecurity Anxiety

Mediation theory holds that environmental stressors influence psychological outcomes through intermediate emotional or cognitive processes, rather than solely via direct effects. Within the Stress and Coping Theory, emotional reactions, including anxiety, are understood as key processes through which stressors affect mental health [4]. In the context of cybersecurity, exposure to cyber threats is an external stressor; the outcome is the emergence of cybersecurity anxiety, an emotional reaction to the appraisal of the threat that, in turn, can undermine mental health. Exposure to cyber threats is often associated with uncertainty, a perceived lack of control, and the potential for personal, financial, or academic damage. These features increase the likelihood that people perceive cyber threats as highly stressful, thereby triggering anxiety. When this fear persists, it can extend beyond the digital realm, adding to overall psychological suffering, anxiety symptomatology, and depression. This aligns with Technology Threat Avoidance Theory, which suggests that the perceived severity of technology threats and vulnerability lead to fear and anxiety that transcend immediate behavioural responses and affect psychological well-being [5]. There is indirect evidence of this mediating pathway in empirical studies. Existing studies show a positive relationship between exposure to cyber threats and technology-related anxiety [10], and that concurrent technology-related anxiety is associated with worse mental health outcomes [8, 11]. However, most studies examine these relationships independently rather than integrated mediation models, especially in university samples. Given that students are heavily dependent on digital platforms to interact and participate in academic activities, cybersecurity anxiety may be a fundamental psychological process that links exposure to cyber threats with mental health. Cyber threat exposure might heighten anxiety by undermining perceptions of digital safety and control, and sustained contact with anxiety compromises emotional well-being. Research on cybersecurity anxiety as a mediator thus provides a more detailed perspective on how cyber threats translate into mental health effects in universities. According to this theoretical and empirical rationale, cybersecurity anxiety should mediate the association between cyber threat exposure and the mental health of university students.

This brings about the last hypothesis:

H4: Cybersecurity anxiety mediates the relationship between cyber threat exposure and mental health among university students.

2.6 Conceptual Framework

The conceptual framework proposes that cyber threat exposure directly influences mental health and indirectly influences mental health through cybersecurity anxiety, which acts as a mediating variable. This framework is grounded in Stress and Coping Theory and supported by Technology Threat Avoidance Theory. Figure 1 presents the study's conceptual framework

3. Methodology

The study adopted a quantitative, cross-sectional survey design to examine the mediating role of cybersecurity anxiety in the relationship between cyber threat exposure and mental health among university students. A survey approach is appropriate because the study focuses on psychological perceptions, emotional responses, and self-reported experiences, which are best captured through standardised instruments. The target population comprised undergraduate and postgraduate students enrolled at the University of Education, Winneba. Students were selected for their high level of engagement with digital technologies and greater exposure to cyber threats in academic and social contexts. They were also selected using a convenience sampling technique, commonly employed in behavioural and mental-health research involving student populations. Eligibility criteria required participants to (a) be currently enrolled as a university student and (b) regularly use digital platforms for academic or personal activities. A total of 563 valid responses were obtained and used for analysis after data screening. This sample size satisfies the minimum requirements for mediation analysis using regression-based or structural equation modelling techniques [14]. Data were collected using a structured online questionnaire distributed through institutional and student communication platforms. Participation was voluntary, and informed consent was obtained from all respondents prior to data collection. Ethical principles of anonymity, confidentiality, and voluntary withdrawal were strictly observed. No personally identifiable information was collected, and data were used solely for academic research purposes. All constructs were measured using validated scales drawn from prior peer-reviewed studies [1, 2, 8, 10]. Responses were recorded on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree), unless otherwise stated. Construct reliability was assessed using Cronbach's alpha, with values of 0.70 or higher considered acceptable. Construct validity was evaluated using confirmatory factor analysis (CFA), with attention to factor loadings, composite reliability, and average variance extracted (AVE). Discriminant validity was assessed using the Fornell–Larcker criterion.

4. Results

4.1 Covariance-based SEM

The relationships among the study variables were examined using covariance-based structural equation modelling (CB-SEM). This technique is widely used for theory testing and confirmation, as it focuses on reproducing the covariance matrix and evaluating overall model fit between observed and latent variables [16, 17]. CB-SEM is particularly appropriate for studies with established theoretical foundations, as it enables rigorous assessment of measurement quality and hypothesised relationships among constructs. In SEM, two main components are evaluated: the measurement model and the structural model. The measurement model examines the relationships between latent constructs and their observed indicators, whereas the structural model assesses relationships among latent constructs and tests the proposed hypotheses.

4.2 Measurement Model Assessment

The measurement model was assessed to establish the reliability and validity of the latent constructs used in the study. As presented in Table 1, the results indicate that all constructs exhibit satisfactory indicator reliability, internal consistency, and convergent validity, thereby supporting their suitability for subsequent structural model analysis. Indicator reliability was first evaluated using standardised factor loadings obtained through confirmatory factor analysis. All measurement items recorded loadings above the recommended threshold of 0.70, ranging from 0.716 to 0.917 [16]. Specifically, Cyber Threat Exposure items loaded between 0.716 and 0.818, Mental Health items ranged from 0.783 to 0.917, and Cyber Security Anxiety items loaded between 0.723 and 0.811. These results indicate that the observed indicators adequately represent their respective latent constructs and that respondents consistently understood and responded to the measurement items. Internal consistency reliability was assessed using Cronbach's alpha, which is the preferred reliability measure in covariance-based SEM. As shown in Table 1, Cronbach's alpha values ranged from 0.823 to 0.923, exceeding the minimum acceptable threshold of 0.70 [18]. These findings confirm that the measurement scales demonstrate strong internal consistency and reliability. Convergent validity was further assessed using the Average Variance Extracted (AVE) criterion. As reported in Table 1, AVE values for all constructs exceeded the recommended benchmark of 0.50, ranging from 0.534 to 0.678 [19]. Notably, Cyber Threat Exposure recorded the highest AVE value (0.678), indicating that its indicators powerfully capture the underlying construct. Overall, these results confirm that each construct accounts for a substantial proportion of the variance in its observed indicators.

Table 1
Reliability and Validity Results

Constructs	Loading of items	Cronbach Alpha	Composite Reliability (CR)	Average variance extracted (AVE)
Cyber threat Exposure		0.843	0.842	0.678
CTE1	0.818			
CTE2	0.790			
CTE3	0.740			
CTE4	0.744			
CTE5	0.716			
Mental Health		0.923	0.924	0.534
MH1	0.783			
MH2	0.849			
MH3	0.917			
MH4	0.858			
MH5	0.812			
MH6	0.837			
Cyber Security Anxiety		0.823	0.827	0.671
CSA1	0.723			
CSA2	0.775			
CSA3	0.772			
CSA4	0.811			
CSA5	0.736			

Discriminant validity was evaluated using the Heterotrait–Monotrait ratio (HTMT) criterion proposed by Henseler et al. [20]. As presented in Table 2, all HTMT values were below the conservative threshold of 0.85, indicating adequate discriminant validity among the constructs. Specifically, the HTMT values between Cyber Threat Exposure and Cyber Security Anxiety (0.543), Cyber Threat Exposure and Mental Health (0.609), and Cyber Security Anxiety and Mental Health (0.701) indicate that the constructs are empirically distinct and do not exhibit multicollinearity or conceptual overlap. From a practical perspective, this distinction is important because it demonstrates that each construct contributes uniquely to explaining the psychological and behavioural outcomes examined in the study. Overall, the measurement model exhibits strong reliability and validity, providing a robust foundation for interpreting the structural relationships among the constructs.

Table 2
Heterotrait – Monotrait Results (HTMT)

Cyber Security Anxiety	CSA	STE	MH
Cyber Threat Exposure	0.543		
Mental Health	0.609	0.701	

4.3 Residual Covariance Matrix

The residual covariance matrix, as shown in Table 3, provides additional diagnostic evidence regarding the extent to which the specified CB-SEM model reproduces the observed relationships among the measured indicators. In covariance-based SEM, residual covariances represent the differences between the observed covariances and those implied by the model, and smaller residuals indicate better model fit. As shown in the residual covariance matrix, most residual values are small in magnitude and clustered near zero, suggesting that the hypothesised measurement and structural models adequately capture the data's covariance structure. Across the indicators of Cyber Security Anxiety, Cyber Threat Exposure, and Mental Health, most residual covariances fall within a narrow range, generally below ± 0.15 , with no systematic pattern of large unexplained covariances. This indicates that the relationships among indicators are primarily accounted for by their respective latent constructs and the specified structural paths. The absence of consistently large residuals within or across constructs suggests that there are no substantial misspecifications due to omitted cross-loadings or missing structural relationships. Some moderately higher residual values are observed between a small number of item pairs, particularly involving Mental Health indicators (MH6 with CSA1 and CTE3) and a few cross-construct item combinations. However, these residuals remain within acceptable limits for applied social science research and appear to be isolated rather than systematic. Such localised residuals may reflect item-specific measurement error or minor overlap in item wording rather than structural deficiencies in the model. Importantly, these residuals do not cluster around a single construct or factor, which would otherwise suggest a more serious misspecification problem. The residual covariance matrix supports the adequacy of the specified CB-SEM model. The generally small and randomly distributed residuals indicate that the model reproduces the observed covariances with reasonable accuracy, reinforcing the conclusions drawn from the global fit indices. Consequently, the residual analysis provides further confirmation that the measurement model (Fig. 2) is well specified and that the structural relationships among Cyber Threat Exposure, Cyber Security Anxiety, and Mental Health are appropriately represented.

Table 3
Residual Covariance Matrix

CSA1	CSA1	CSA2	CSA3	CSA4	CSA5	CTE1	CTE2	CTE3	CTE4	CTE5	MH1	MH2	MH3	MH4	MH5	MH6
	0.000	-0.013	0.045	0.055	0.035	-0.109	-0.095	-0.108	0.021	0.053	-0.125	-0.152	-0.136	-0.121	-0.111	-0.185
CSA2	-0.013	-0.000	-0.054	0.035	0.014	-0.002	0.066	-0.010	0.083	0.109	-0.034	0.062	0.061	-0.032	0.049	-0.055
CSA3	0.045	-0.054	-0.000	0.005	0.001	-0.004	0.011	-0.012	0.118	0.114	-0.058	0.048	0.049	0.005	0.015	-0.021
CSA4	0.055	0.035	0.005	-0.000	-0.128	-0.000	0.004	-0.009	0.096	0.038	-0.025	0.041	0.062	0.083	0.026	0.045
CSA5	0.035	0.014	0.001	-0.128	-0.000	-0.046	-0.037	-0.016	0.022	0.000	-0.050	0.076	0.093	0.080	0.043	0.036
CTE1	-0.109	-0.002	-0.004	-0.000	-0.046	-0.000	-0.008	0.048	-0.045	0.029	0.039	0.012	0.001	0.068	-0.013	-0.044
CTE2	-0.095	0.066	0.011	0.004	-0.037	-0.008	-0.000	0.006	0.039	-0.030	-0.025	-0.055	-0.029	0.061	-0.035	-0.052
CTE3	-0.108	-0.010	-0.012	-0.009	-0.016	0.048	0.006	-0.000	-0.013	0.003	-0.048	-0.082	-0.052	-0.039	-0.051	-0.159
CTE4	0.021	0.083	0.118	0.096	0.022	-0.045	0.039	-0.013	-0.000	-0.081	0.070	0.061	0.059	0.111	0.004	0.019
CTE5	0.053	0.109	0.114	0.038	0.000	0.029	-0.030	0.003	-0.081	-0.000	0.088	0.047	0.103	0.097	0.002	0.004
MH1	-0.125	-0.034	-0.058	-0.025	-0.050	0.039	-0.025	-0.048	0.070	0.088	-0.000	-0.039	0.013	-0.076	0.085	0.039
MH2	-0.152	0.062	0.048	0.041	0.076	0.012	-0.055	-0.082	0.061	0.047	-0.039	0.000	-0.016	0.003	0.007	0.039
MH3	-0.136	0.061	0.049	0.062	0.093	0.001	-0.029	-0.052	0.059	0.103	0.013	-0.016	-0.000	0.008	-0.016	0.009
MH4	-0.121	-0.032	0.005	0.083	0.080	0.068	0.061	-0.039	0.111	0.097	-0.076	0.003	0.008	0.000	0.013	-0.026
MH5	-0.111	0.049	0.015	0.026	0.043	-0.013	-0.035	-0.051	0.004	0.002	0.085	0.007	-0.016	0.013	0.000	-0.014
MH6	-0.185	-0.055	-0.021	0.045	0.036	-0.044	-0.052	-0.159	0.019	0.004	0.039	0.039	0.009	-0.026	-0.014	0.000

4.4 Principal Component Analysis

Table 4 presents the results of the Principal Component Analysis (PCA), summarising the eigenvalues, proportion of variance explained, and cumulative variance across the extracted components. PCA was conducted to examine the underlying data structure and assess the extent to which fewer components could represent the observed variables. The results indicate a clear dominance of the first few components in explaining the total variance in the dataset. The first principal component recorded a very high eigenvalue of 7.457. It accounted for 46.6% of the total variance, suggesting that a single underlying dimension captures a substantial proportion of the information contained in the original variables. This dominant component reflects strong commonality among the measured variables, indicating that they share considerable variance. The second and third components had eigenvalues of 1.782 and 1.468, explaining 11.1% and 9.2% of the variance, respectively. When combined with the first component, the first three components cumulatively explain 66.9% of the total variance, which exceeds the commonly recommended threshold for satisfactory variance explanation in social science research.

Table 4
Principal Component Analysis (PCA)

Component 1	Eigenvalue	Variance proportion	Variance cumulative
	7.457	0.466	0.466
Component 2	1.782	0.111	0.577
Component 3	1.468	0.092	0.669
Component 4	0.708	0.044	0.713
Component 5	0.607	0.038	0.751
Component 6	0.598	0.037	0.789
Component 7	0.515	0.032	0.821
Component 8	0.487	0.030	0.851
Component 9	0.470	0.029	0.881
Component 10	0.374	0.023	0.904
Component 11	0.346	0.022	0.926
Component 12	0.302	0.019	0.945
Component 13	0.277	0.017	0.962
Component 14	0.241	0.015	0.977
Component 15	0.201	0.013	0.990
Component 16	0.166	0.010	1.000

Applying the Kaiser [21] criterion, which recommends retaining components with eigenvalues greater than 1.0, the results indicate retaining three principal components. Components four through sixteen all recorded eigenvalues below 1.0 and each explained less than 5% of the total variance individually, indicating diminishing explanatory power. Although the cumulative variance continues to increase with the inclusion of additional components, reaching 71.3% by the fourth component and 78.9% by the sixth component, the marginal gain in explained variance beyond the third component is relatively small. Overall, the PCA results indicate that the data structure is adequately represented by a small number of principal components, with the first three capturing most of the variance. This pattern supports the presence of an underlying multidimensional structure and indicates that the observed variables are sufficiently interrelated to justify dimension reduction. The dominance of the first component further suggests a strong general factor underlying the measures, while the subsequent components contribute additional, but progressively smaller, unique explanatory power. These findings provide empirical support for the factor structure assumed in the subsequent measurement and structural analyses.

The scree plot provides a visual representation of the eigenvalues associated with each principal component and offers additional support for determining the appropriate number of components to retain. As shown in the scree plot, there is a steep decline in eigenvalues from the first to the second component, followed by a more gradual decrease thereafter. The first component exhibits a substantially higher eigenvalue than all subsequent components, indicating that it captures a large proportion of the total variance in the dataset. A noticeable inflexion point, or “elbow,” occurs around the third component, after which the curve begins to flatten and the eigenvalues level off. This pattern suggests that the first three components account for a substantial proportion of the variance, whereas the remaining components contribute relatively little. Components beyond the third fall below the eigenvalue threshold of 1.0, as indicated by the horizontal reference line, and display a shallow slope, reflecting diminishing returns in terms of variance explained. This visual evidence is consistent with the Kaiser criterion. It aligns closely with the PCA results reported in Table 4, in which only the first three components have eigenvalues greater than one, and together they account for approximately 66.9% of the total variance. The scree plot confirms that retaining three principal components is both statistically and conceptually justified. The sharp drop followed by a clear levelling-off indicates that a limited number of components can adequately summarise the underlying data structure. In contrast, additional components primarily represent random noise or trivial variance. These findings strengthen the decision to retain three components for further analysis and provide empirical support for the dimensional structure assumed in subsequent factor and structural modelling.

4.5 Structural Model Assessment

The structural model was evaluated using covariance-based structural equation modelling (CB-SEM) to examine the hypothesised relationships among Cyber Threat Exposure, Cyber Security Anxiety, and Mental Health. In CB-SEM, the assessment of the structural model focuses primarily on the significance and magnitude of standardised path coefficients, as well as the coefficient of determination (R^2), which indicates the model's explanatory power [16, 17]. The results of the structural model are summarised in Table 5. As reported in Table 4, Cyber Threat Exposure has a significant positive total effect on Cyber Security Anxiety ($\beta = 0.463$), indicating that increased exposure to cyber threats substantially heightens individuals' anxiety related to cybersecurity issues. Cyber Threat Exposure also shows a substantial direct effect on Mental Health ($\beta = 0.582$), suggesting that higher levels of exposure are associated with poorer mental health outcomes. In addition, Cyber Security Anxiety demonstrates a positive effect on Mental Health ($\beta = 0.284$), indicating that anxiety arising from cybersecurity concerns contributes meaningfully to mental health challenges. These findings collectively support the proposed theoretical relationships and highlight the central role of cyber-related stressors in shaping psychological well-being.

Table 5
Coefficient of determination

Constructs	Total Effect	R ²	Adjusted R ²
CSA -> MH	0.284		
CTE-> CSA	0.463		
CTE-> MH	0.582		
		0.321 (CSA)	0.558 (MH)
Note: CSA; Cyber Security Anxiety, CTE; Cyber threat Exposure, MH; Mental Health			

The model's explanatory power was assessed using the coefficient of determination (R^2). As shown in Table 4, Cyber Threat Exposure accounts for 32.1% of the variance in Cyber Security Anxiety ($R^2 = 0.321$), indicating moderate explanatory power. Furthermore, Cyber Threat Exposure and Cyber Security Anxiety together explain 55.8% of the variance in Mental Health ($R^2 = 0.558$), which can be considered substantial according to commonly accepted CB-SEM benchmarks, where R^2 values of approximately 0.25, 0.50, and 0.75 represent weak, moderate, and vigorous explanatory power, respectively [16]. These results suggest that the model provides a robust explanation of mental health outcomes within the context of cyber threat exposure and anxiety. From a practical perspective, the findings imply that cyber threat exposure not only directly affects mental health but also indirectly influences it through increased cybersecurity anxiety. The relatively high R^2 value for Mental Health indicates that the combined effects of Cyber Threat Exposure and Cyber Security Anxiety account for a substantial proportion of variance in psychological well-being. Overall, the structural model demonstrates strong explanatory power and supports the theoretical framework underpinning the study, thereby confirming its suitability for understanding the mental health implications of cyber-related risks.

4.6 Model Fitness

Model fitness was assessed using several global goodness-of-fit indices commonly applied in covariance-based structural equation modelling (CB-SEM) to evaluate how well the hypothesised model reproduces the observed covariance matrix. As shown in Table 6, model fit was examined using the chi-square statistic (χ^2), the ratio of chi-square to degrees of freedom (χ^2/df), the Root Mean Square Error of Approximation (RMSEA) with its confidence intervals, the Standardized Root Mean Square Residual (SRMR), and incremental fit indices including the Goodness-of-Fit Index (GFI), Normed Fit Index (NFI), Tucker–Lewis Index (TLI), and Comparative Fit Index (CFI). These indices collectively provide a comprehensive assessment of absolute, incremental, and parsimonious model fit [16, 17]. As reported in Table 5, the estimated model produced a chi-square value of 259.780 with 101 degrees of freedom, which is statistically significant ($p < 0.001$). While the chi-square test is sensitive to sample size, particularly in large-sample models, the relative chi-square statistic (χ^2/df) provides a more practical indicator of model fit. The obtained χ^2/df value of 1.572 falls well below the recommended threshold of 3.0, indicating a good fit between the hypothesised model and the observed data. This suggests that the discrepancy between the sample covariance matrix and the model-implied covariance matrix is within acceptable limits.

Further evidence of satisfactory model fit is provided by the RMSEA value of 0.072, which falls within the acceptable range of 0.08 or below. The 90% confidence interval for RMSEA ranges from 0.051 to 0.083, indicating a reasonable approximation of the population covariance matrix and supporting the stability of the model fit. In addition, the SRMR value of 0.058 is below the recommended cut-off of 0.08, suggesting minimal residual differences between observed and predicted correlations. Together, these absolute fit indices indicate that the model adequately captures the underlying structure of the data. With respect to incremental fit indices, the GFI value of 0.802 indicates an acceptable overall model fit given the model's complexity. Although the NFI (0.713), TLI (0.634), and CFI (0.745) values fall below the more stringent cut-off of 0.90, such outcomes are not uncommon in complex models involving moderation effects and multiple parameters, particularly in applied social science research. These values nonetheless suggest that the hypothesised model provides a meaningful improvement over the null model. The parsimony-adjusted indices, including the AGFI (0.668) and PGFI (0.670), further indicate that the model achieves a reasonable balance between explanatory power and model complexity.

Table 6
Model Fitness

Parameters	Estimated model
Chi-square	259.780
Number of model parameters	35.000
Number of observations	303.000
Degrees of freedom	101.000
P value	0.000
ChiSqr/df	1.572
RMSEA	0.072
RMSEA LOW 90% CI	0.051
RMSEA HIGH 90% CI	0.083
GFI	0.802
AGFI	0.668
PGFI	0.670
SRMR	0.058
NFI	0.713
TLI	0.634
CFI	0.745
AIC	329.780
BIC	359.761
Source: CB SEM	

From a practical perspective, the overall pattern of fit indices suggests that the empirical data adequately support the hypothesised structural relationships among the study constructs. The acceptable absolute and parsimonious fit measures indicate that the model reflects systematic relationships rather than random variation. Consequently, the satisfactory model fit provides confidence in the validity of the estimated structural paths and supports the robustness of the proposed conceptual framework. This implies that the model offers a credible representation of the underlying relationships among the constructs and provides a sound basis for interpreting the study's substantive findings.

4.7 Hypothesis Test

Path coefficients assess the degree of relevance of one variable to another using the p-value (significance level), β -value (direction of the path), and T-value (hypothesis testing) [22, 23, 24]. All hypotheses with p-values less than 0.05 ($p < .005$) are considered statistically significant, and T-values more than 1.99 are supported (Hair et al., 2019). Table 6 and Fig. 4 show the supported hypotheses, including H1, H2, H3, and H4. The hypotheses are supported because the T-values exceed 1.99 and the p-values are less than 0.05.

Table 6
Hypothesis Testing

Structural Relationship	Hypotheses	Standardised Beta (B)	T-Statistics (t-Value > 1.96)	p-Values	Status of the Hypothesis
Direct effect:					
Cyber threat exposure → Mental health	H1	0.450	5.270	0.000	Supported
Cyber threat exposure → Cyber security anxiety	H2	0.463	6.631	0.000	Supported
Cybersecurity Anxiety → Mental Health	H3	0.284	2.999	0.003	Supported
Indirect Effect:					
Cyber threat exposure → Cyber Security Anxiety → Mental Health	H4	0.132	2.568	0.011	Supported
Note: CSA; Cyber Security Anxiety, CTE; Cyber threat Exposure, MH; Mental Health					

5. Discussion of Results

The results reported in Table 6 are empirically high and align with the theoretical framework on which the study was conducted. Overall, the findings are consistent with Stress and Coping Theory and Technology Threat Avoidance Theory, in that cyber threat exposure can be regarded as a salient environmental stressor, cybersecurity anxiety is a primary response of the emotional system, and mental health is a psychological outcome. Regarding the direct correlation between cyber threat exposure and mental health (H1), the results indicate a positive and statistically significant association ($b = 0.450$, $t = 5.270$, $p < 0.001$). The results confirm the hypothesis that greater exposure to cyber threats is associated with poorer mental health among university students. Based on the Stress and Coping Theory, this outcome supports the idea that exposure to cyber threats is a stressor that may adversely affect psychological well-being when it is perceived as a threat and as challenging to manage. This relationship is strong enough to imply that recurring exposure to cyberbullying, phishing, identity theft, or unauthorised access to their accounts can weaken the emotional integrity of students in the long run. This result aligns with previous facts of empirical research to indicate that cyber-victimisation and risk exposure online correlate with increased stress levels, anxiety, and psychological distress among student groups [2, 3]. The H1 further supports the conclusion that cyber threats are a significant risk factor for mental health in digitally intensive university settings.

The outcomes also reveal a substantial and significant effect of cyber threat exposure on cybersecurity anxiety (H2); the standardised beta coefficient is 0.463 ($t = 6.631$, $p < 0.001$). This observation is entirely consistent with Stress and Coping Theory and Technology Threat Avoidance Theory. The Stress and Coping Theory indicates that anxiety develops when persons perceive the environmental demands as threatening and they feel they have inadequate resources to cope with it. Cyber threats are unpredictable, technically challenging, and difficult to manage; therefore, they pose the most significant risk of eliciting panic. Technology Threat Avoidance Theory further elaborates on this relationship, stating that perceived severity and vulnerability to technology-related threats are antecedents of fear and anxiety. This fact is evidenced by a significant correlation of H2, which proves that the exposure to cyber threats is not an incidental background risk but a direct psychological antecedent of cybersecurity anxiety in the minds of university students, which is consistent with previous results by Hadlington [8], Boss et al. [10], and Shillair et al. [9].

Regarding H3, the findings show that there is a significant positive correlation between cybersecurity anxiety and mental health ($b = 0.284$, $t = 2.999$, $p = 0.003$), and the higher the level of cybersecurity anxiety, the worse the mental health condition is. This observation confirms the theoretical assumption that the proximal mechanism through which stressors affect psychological well-being is sustained anxiety. Under the Stress and Coping Theory, unresolvable or persistent anxiety translates to inefficient coping and is likely to lead to emotional tension and psychological-health complications. The outcome also aligns with Technology Threat Avoidance Theory, which posits that fear and anxiety arising from perceived technology threat may not be confined to direct avoidance behaviours but also influence other aspects of psychological functioning. This is empirically consistent based on the literature that indicates that technology-related anxieties are linked to higher levels of distress, anxiety symptoms, and lower well-being in digitally dependent groups, especially among students [8, 11]. The evidence in favour of H3 specifies cybersecurity anxiety as a key psychological factor that affects the mental health of students.

Above all, the mediating effect of cybersecurity anxiety on the correlation between cyber threat exposure and mental health is supported by the indirect effect result (H4). The indirect effect of cyber threat exposure on mental health via cybersecurity anxiety is statistically significant ($b = 0.132$, $t = 2.568$, $p = 0.011$), indicating that cybersecurity anxiety is a partial mediator of this relationship. The presented finding provides solid empirical support for the proposed mediation model and aligns with mediation theory and Stress and Coping Theory. It implies that the exposure to cyber threats can not only have a direct but also an indirect negative impact on mental health, as it leads to the development of anxiety towards cybersecurity and, consequently, a decrease in psychological well-being. This is consistent with the theoretical evidence that emotional reactions like anxiety are important processes by which environmental stressors are converted to mental-health actions. The mediation result also continues Technology Threat Avoidance Theory, showing that anxiety caused by perceived technology threats has secondary effects on mental health, rather than being limited to direct behavioural effects (avoidance or heightened vigilance). Although previous research has analysed the direct correlations between exposure to cyber threats and anxiety and between anxiety and mental health, this research incorporates these into one explanatory model. The findings can hence be added to the literature to provide the empirical confirmation of cybersecurity anxiety as a key psychological process through which exposure to cyber threats is connected to mental health in university students. Taken together, the results provide solid evidence for all four hypotheses and offer a logical theoretical account grounded in Stress and Coping Theory and Technology Threat Avoidance Theory. Exposure to cyber threats can be a significant source of stress in the digital lives of university students. Anxiety as a response to cybersecurity threats may be considered a critical expression of stress, and mental health may become the ultimate psychological consequence of the continued presence of these stressors and anxiety. These findings imply that cyber threat exposure and cybersecurity anxiety are critical issues that should be considered when mitigating and advancing student mental health in the rapidly digitalising academia.

6. Conclusion

This study has examined the mediating role of cybersecurity anxiety in the relationship between exposure to cyber threats and mental health among university students. Drawing on the Stress and Coping Theory and the Technology Threat Avoidance Theory, the results provide strong empirical evidence that exposure to cyber threats is a salient source of psychological stress in digitally intensive academic settings. The findings suggest that students exposed to high levels of cyber threats are susceptible to developing cybersecurity-related anxiety, which, in turn, negatively affects mental health outcomes. In this research, cybersecurity anxiety serves as an effective psychological mediator of the effect of exposure to cyber threats on mental health. Therefore, cyber threats directly affect students through acute stress reactions and indirectly through prolonged emotional reactions linked to the perception of digital vulnerability and loss of control. The model demonstrates significant explanatory power, with cyber threat exposure and cybersecurity anxiety accounting for a substantial share of the variability in students' mental health outcomes. Overall, the research highlights the growing consensus that cybersecurity threats should be regarded not only as a technological or institutional challenge but also as a key determinant of student well-being. With the increasing digitalisation of learning, administration, and communication processes in higher education institutions, a detailed understanding of the psychological implications of cyber risks is increasingly vital to maintaining an effective system of student support.

6.1 Theoretical Implication

This study contributes to theory development in three salient ways. To begin with, it applies the Stress and Coping Theory to the contemporary digital milieu, empirically demonstrating that cyber threats function as current environmental stressors, triggering affective reactions that impact psychological health. As a result, the theory's scope is extended beyond conventional environmental stress situations into technology-affiliated risk contexts. Secondly, the article advances the Technology Threat Avoidance Theory by showing that the perception of technological threats not only elicits behavioural protective responses but also generates universal psychological effects. By exposing the mental health consequences of cybersecurity anxiety, the study broadens TTAT from a purely behavioural protection model to one that also accounts for psychosocial risk aspects. Thirdly, the research strengthens mediation-based psychological process modelling in digital risk scholarship. Empirical evidence identifying cybersecurity anxiety as a critical mediating variable offers a more nuanced explanation of how exposure to cyber threats translates into mental health outcomes. This contributes to the body of literature on digital well-being by characterising cybersecurity anxiety as a domain-specific emotional reaction with broad psychological implications.

6.2 Practical Implication

The results have important implications for universities, student support systems, and policymakers. To begin with, institutions need to incorporate cybersecurity education and mental health services for students. Psychological coping training should be included in the cybersecurity curriculum to help students overcome fear, uncertainty, and anxiety related to cyber threats. Secondly, cybersecurity anxiety should be recognised as a new determinant of student stress within university counselling services. Cyber-intervention mental health interventions can incorporate digital stress-management activities and cyber-resilience strategies based on cyber-risk exposures. Thirdly, institutional cybersecurity communication needs improvement. By publicly reporting cybersecurity practices, perceived vulnerability can be reduced and trust in institutional digital systems can be increased. Fourthly, cybersecurity risk management in student well-being models should be institutionalised by policymakers in higher education. Cybersecurity should be part of student welfare governance as more and more digital platforms become essential to the learning environment. Lastly, the results reveal the need to involve IT departments, student affairs units, and mental health professionals in multidisciplinary efforts to develop holistic strategies for digital safety.

6.3 Limitations

Despite its contributions, several limitations should be acknowledged. To begin with, a cross-sectional design does not inherently permit establishing causal relations, and longitudinal studies are also necessary to analyse how exposure to cyber threats is modulated over time and how it affects mental health. Second, convenience sampling can be problematic when generalising results to larger groups of students; future inquiries should lean more towards multi-institutional and probability-based sampling. Third, self-report measures subject the study to response bias; future studies could combine objective cybersecurity incident indicators with tested clinical mental health measures. Fourth, the research was conducted in a single institutional setting, which might limit its cultural and institutional generalisability. Lastly, the current study considered only cybersecurity anxiety as a mediating variable; other psychosocial processes can also have an intervening effect on the association between cyber threat exposure and mental health outcome.

6.4 Future Research Directions

Future research should build on this study in several important ways. Longitudinal studies will be needed to clarify how exposure to cyber threats and the ensuing anxiety about cybersecurity change over time, and how they affect mental health outcomes in the long term. Further research should investigate other mediating and moderating factors, including digital literacy, cybersecurity self-efficacy, institutional trust, and social support. Cross-country and cross-organisational studies would help identify contextual differences in cyber-risk exposure and psychological reactions. Intervention-based studies must evaluate the effectiveness of cybersecurity education, resilience training, and institutional protection in reducing cybersecurity anxiety and improving mental health outcomes. Future research may also explore subgroup differences, especially among digitally vulnerable groups of students. Lastly, measurement validity could be strengthened by using mixed-methods approaches that combine survey data with objective records of cyber incidents, thereby improving theoretical development.

Declarations

Acknowledgements: The team sincerely appreciates the participants' time, effort, and willingness to contribute to this study. Your involvement was invaluable, and we are truly grateful for your support.

Author contributions: D.O conceptualized the research topic, conducted the literature review, and developed the conceptual framework for the study. S.O.M performed the data analysis and was responsible for the interpretation and discussion of the study's findings.

Funding: None.

Ethics Approval declaration in the manuscript

The ethics committee in the university was consulted and approved. The methods followed in this research follow the concepts of the Declaration of Helsinki. This research was permitted by the university to proceed through the questionnaire and the methodology used. All individual participants who were involved in the study gave informed consent. Every author has read the final manuscript and has given his consent to submit it to publication.

Competing Interests: The authors declare no competing interests in the study

Clinical trial number: Not applicable.

Consent to Publish declaration: Not applicable

References

1. Luo, Q., Wu, N., Huang, L.: Cybervictimization and cyberbullying among college students. *Frontiers in Psychology* (2023). <https://doi.org/10.3389/fpsyg.2023.1067165>
2. Rahman, T., Hossain, M.M., Bristy, N.N., Hoque, M.Z., Hossain, M.M.: Influence of cyber-victimization and other factors on depression and anxiety among university students in Bangladesh. *Journal of Health, Population and Nutrition* 42(1), 119 (2023). <https://doi.org/10.1186/s41043-023-00469-0>
3. Arif, A., Qadir, M.A., Martins, R.S., Khuwaja, H.M.A.: The impact of cyberbullying on mental health outcomes amongst university students: A systematic review. *PLOS Mental Health* 1(6), e0000166 (2024)
4. Lazarus, R.S., Folkman, S.: Stress, appraisal, and coping. Springer, New York (1984)
5. Liang, H., Xue, Y.: Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly* 33(1), 71–90 (2009)
6. Tremolada, M., Bonichini, S., Taverna, L.: Coping strategies and perceived support in adolescents and young adults: Predictive model of self-reported cognitive and mood problems. *Psychology* 7, 1858–1871 (2016)
7. Wang, H., Zhang, S., Sun, N., Qi, S., Yi, X.: Online risk exposure and anxiety among college students in China: The chain mediating role of negative attribution and interpersonal security. *PLOS ONE* 20(3), e0319700 (2025)
8. Hadlington, L.: Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cyber behaviours. *Heliyon* 3(7), e00346 (2017)
9. Shillair, R., Esteve-González, P., Dutton, W.H., Creese, S., Nagyfejeo, E., von Solms, B.: Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security* 119, 102756 (2022)
10. Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P.: What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviours. *MIS Quarterly* 39(4), 837–864 (2015)
11. Shandler, R., Gross, M.L., Canetti, D.: Cyberattacks, psychological distress, and military escalation: An internal meta-analysis. *Journal of Global Security Studies* 8(1), ogac042 (2023)
12. Opoku, D., Donkor, C., Yeboah, J.N.O., Quagrainie, L.: Navigating the relationship between social media use and mental health in the digital age. *Discover Mental Health* 5(1), 149 (2025)
13. Budimir, S., Fontaine, J.R., Huijts, N.M., Haans, A., Loukas, G. and Roesch, E.B.: Emotional reactions to cybersecurity breach situations: scenario-based survey study. *Journal of medical Internet research*, 23(5), p.e24879 (2021)
14. Hayes, A.F.: Introduction to mediation, moderation, and conditional process analysis, 2nd edn. Guilford Press, New York (2018)
15. Auerbach, R.P., Mortier, P., Bruffaerts, R., et al.: Mental disorder prevalence among college students worldwide. *World Psychiatry* 21(1), 129–140 (2022)
16. Hair, J.F., Astrachan, C.B., Moisesescu, O.I., Radomir, L., Sarstedt, M., Vaithilingam, S., Ringle, C.M.: Executing and interpreting applications of PLS-SEM: Updates for family business researchers. *Journal of Family Business Strategy* 12(3), 100392 (2021)
17. Kline, R.B.: Principles and practice of structural equation modeling. Guilford Press, New York (2023)
18. Nunnally, J.C., Bernstein, I.H.: Psychometric theory, 3rd edn. McGraw-Hill, New York (1994)
19. Fornell, C., Larcker, D.F.: Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18(1), 39–50 (1981)
20. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modelling. *Journal of the Academy of Marketing Science* 43(1), 115–135 (2015)
21. Kaiser, H.F.: Coefficient alpha for a principal component and the Kaiser–Guttman rule. *Psychological Reports* 68(3), 855–858 (1991)
22. Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M.: When to use and how to report the results of PLS-SEM. *European Business Review* 31(1), 2–24 (2019)
23. Gil, M.T., Jacob, J.: The relationship between green perceived quality and green purchase intention: A three-path mediation approach using green satisfaction and green trust. *International Journal of Business Innovation and Research* 15(3), 301–319 (2018)
24. Tutu-Boahene, B., Oduro Owusu, S., Gil, M.T.: Idea creation and concept development in family business sustainability: The mediating role of couples' relationships. *Journal of the International Council for Small Business*, 1–31 (2026)

Figures

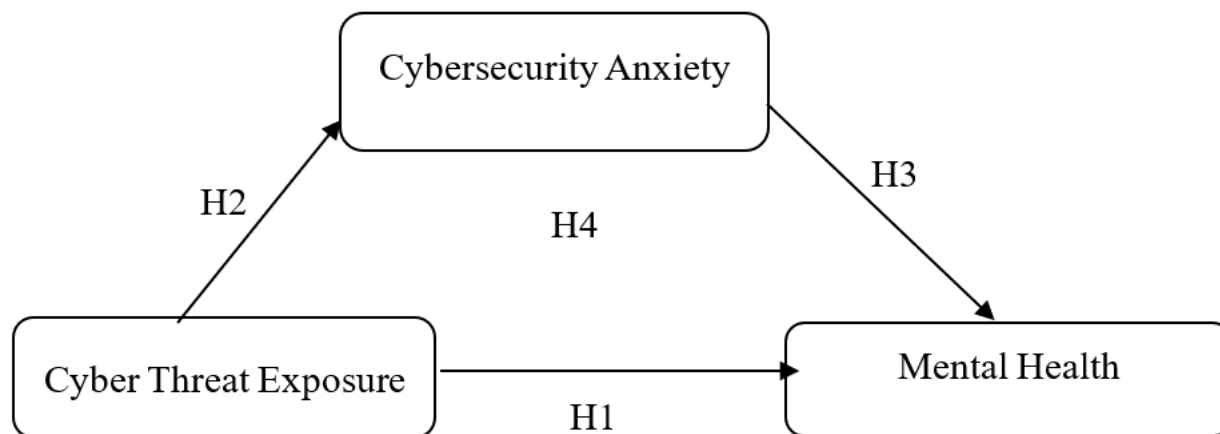


Figure 1

Study model

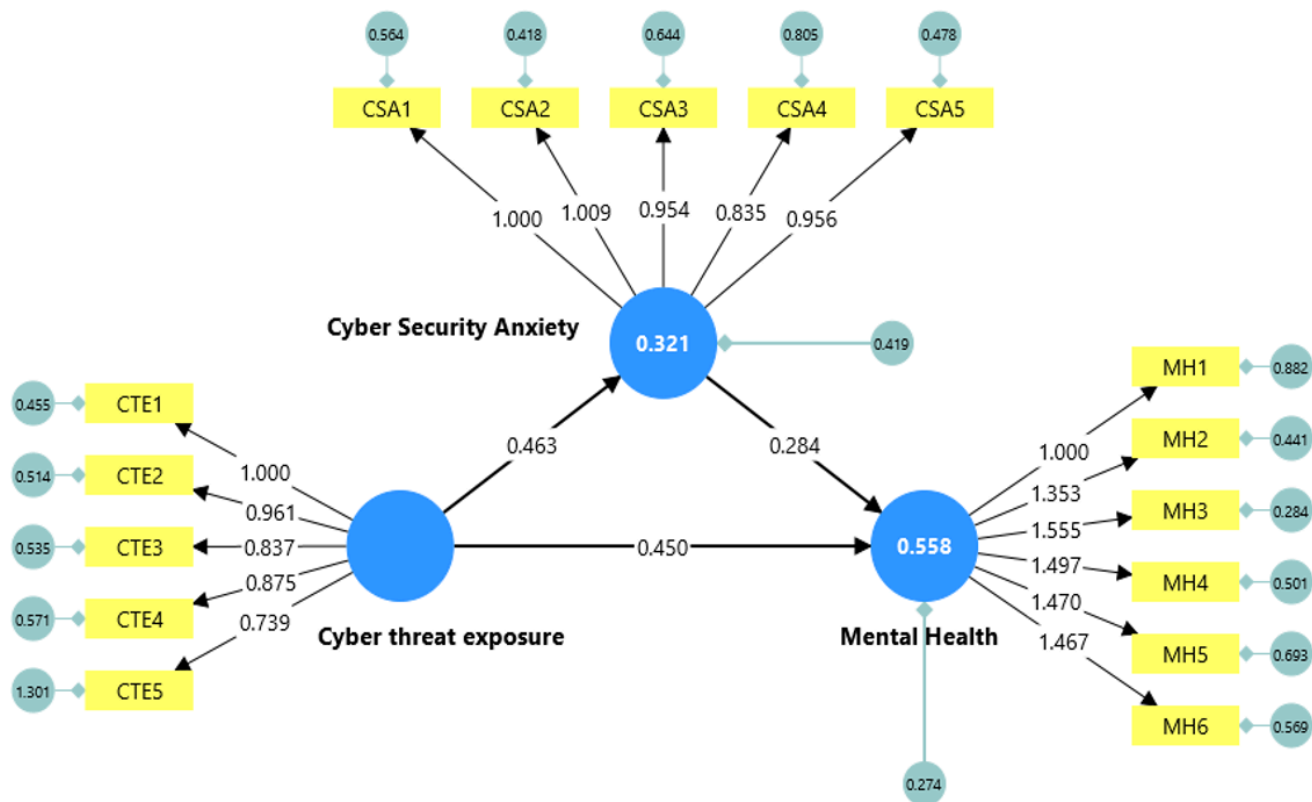


Figure 2

CB SEM Measurement model output

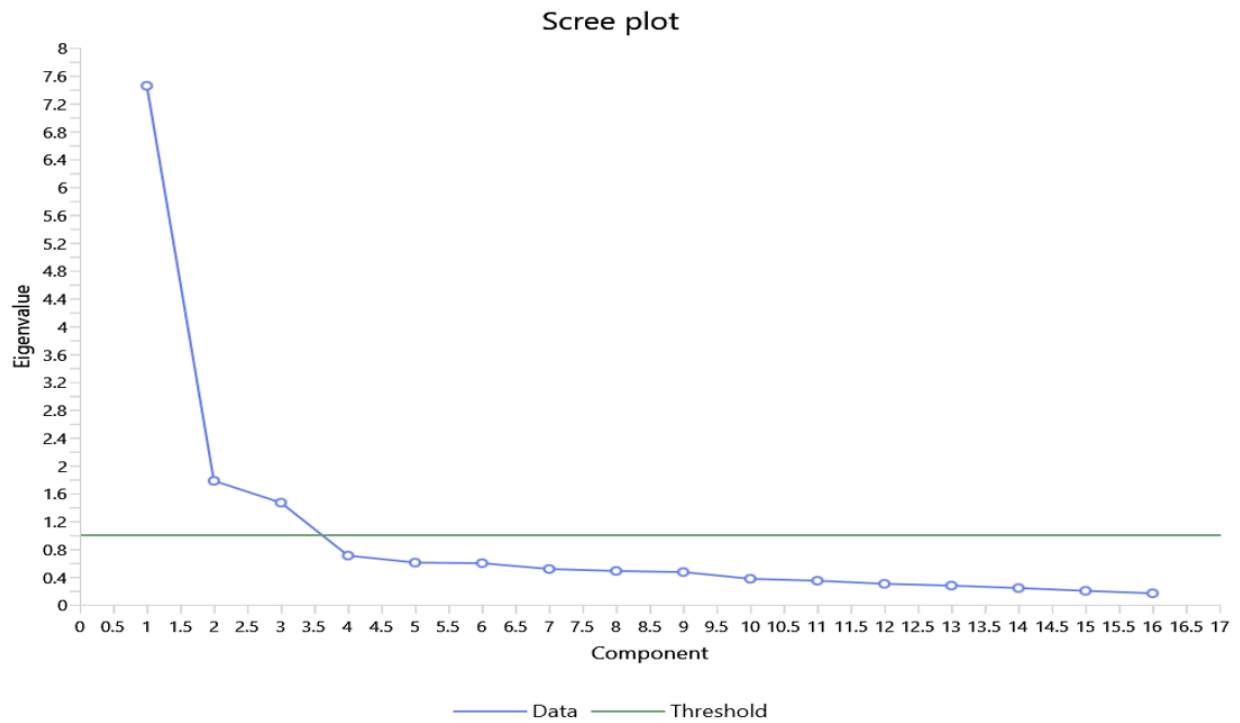


Figure 3

Scree Plot

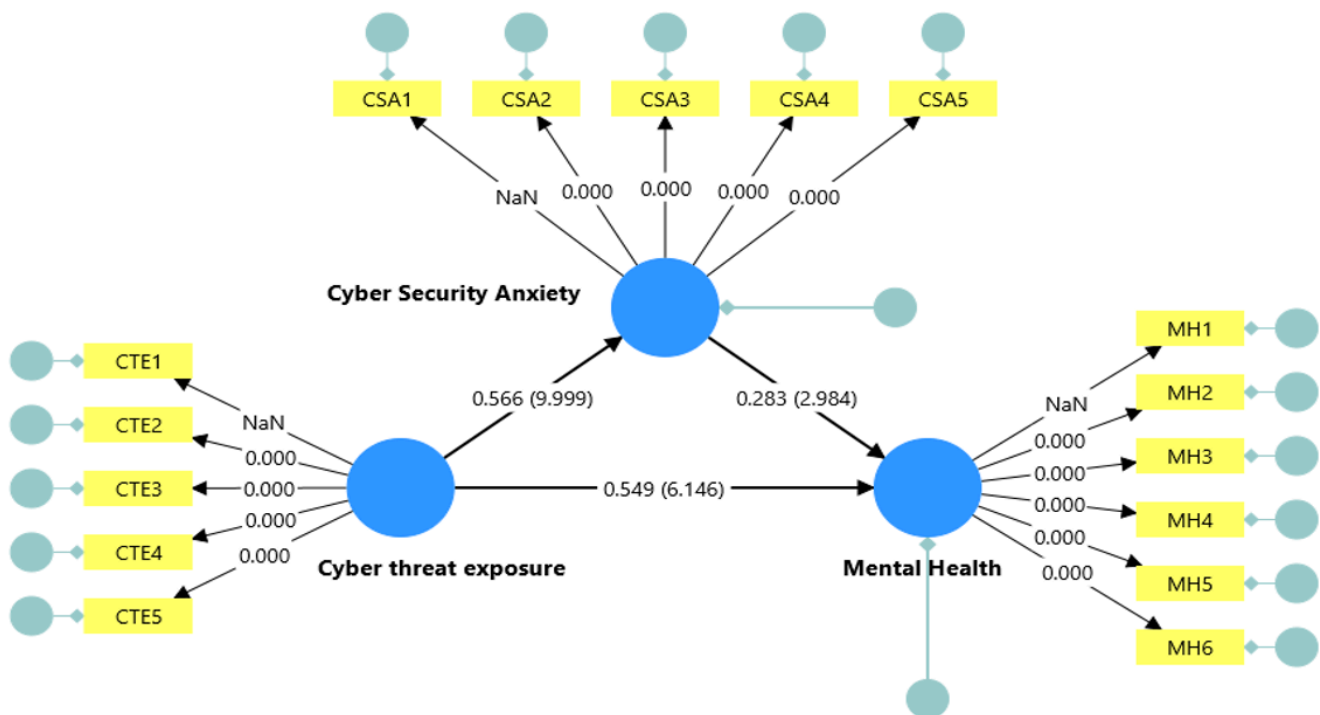


Figure 4

CB SEM Structural model Output