ENHANCING UNIVERSITY CYBERSECURITY SUSTAINABILITY AND EFFECTIVENESS BY APPLYING ACCOUNTANTS' FORENSIC ACCOUNTING, DIGITAL INTELLIGENCE AND MORAL INTELLIGENCE

Assoc.Prof.PhD. Pham Quang Huy* - MSc. Vu Kien Phuc*

Abstract: ***The current study sets its sight to delve into the impact of digital intelligence (DI) and moral intelligence (MI) on cybersecurity performance (CYP) in higher educational institutions (HEIs). This study also aims to investigate the mediating effect of digital forensic accounting (DFA) in the relationship between DI, MI, and CYP. The structural equation modeling was employed with the support of AMOS 28 to analyze the statistical data collected from the sample of accountants in public sector organizations. The results revealed that both DI and MI significantly and positively impact CYP. Additionally, DFA was corroborated to partially mediate the relationships between DI, MI and CYP. Based on these analysis results, some policy implications have been proposed to help improve and enhance CYP in HEIs.***

• Keywords: *cybersecurity, digital intelligence, forensic accounting, moral intelligence.*

Date of receipt: 26th Feb., 2025
Date of delivery revision: 23th Mar., 2025
Date of receipt revision: 15th Apr., 2025
Date of approval: 28th May, 2025
DOI: https://doi.org/10.71374/jfar.v25.i3.11

1. Introduction

Cybersecurity is becoming vital as the utilization of digital technology expands. Cybersecurity can be understood as the collection of methods, techniques, frameworks, and resources employed to safeguard systems within cyberspace. Higher education institutions (HEIs) are susceptible to cyberattacks due to their storage of substantial quantities of personal data pertaining to students, faculty, and staff, as well as data associated with academic and funding activities, and financial information.

Recently, the frequency of cyberattacks targeting higher education institutions has escalated, resulting in the theft and exploitation of data belonging to students, faculty, and staff for illicit reasons. Consequently, information security in higher education institutions is garnering heightened scrutiny, as they must safeguard sensitive data and critical digital assets from both external and internal attacks. In this context, digital forensics has emerged as a viable option in the digital era, garnering significant interest from numerous scholars and organizations.

Research indicates that personnel frequently represent the most vulnerable element in cybersecurity, leading to numerous security breaches within organizations. Moreover, inadequate employee understanding and adherence are recognized as issues that adversely affect organizational cybersecurity. Threats frequently emerge from employees inadvertently or deliberately revealing critical information. Recently, researchers have concentrated on examining the interplay between human-related elements, including cognition, emotion, and behavior, and cybersecurity. Nazaripour and Zakizadeh (2025) assert that employees possessing innovative abilities will foster competitive advantages within firms in the present day. Intelligence encompasses the conduct and efficacy of individuals, as well as their capacity to acquire knowledge in many contexts. Consequently, intelligence is crucial for comprehending, analyzing, processing, and recreating information. This study concentrates on two specific forms of intelligence: digital intelligence and moral intelligence. The aim of this study is to examine the possible influence of digital intelligence (DI) and moral intelligence (MI) on the implementation of digital forensic accounting (DFA) to augment cybersecurity performance (CP) in HEIs. The primary objectives of the research are to analyze the stated reasons through the systematic development of research questions.

RQ1. To what extent does DI impact CSP?

RQ2. To what extent does MI impact CSP?

RQ3. Does DFA mediate the relationships between DI and CSP as well as MI and CSP?

** University of Economics Ho Chi Minh City; corresponding author: pquanghuy@ueh.edu.vn*

2. Literature review

2.1. A contingent resource-based view

The resource-based view posits that businesses can achieve competitive advantage by cultivating resource bundles. These resources comprise assets and capabilities, which may be either tangible or intangible. The literature presents numerous instances of analytical resources, encompassing analytical systems and the integration of personnel, data-analysis methodologies, and technologies that facilitate evidence-based decision-making for company executives. The resource-based view paradigm, while prevalent in existing literature, is seen as fundamentally static in nature (Ling-yee, 2007). This indicates that the resource-based paradigm is insufficient in recognizing and elucidating the circumstances under which capabilities hold the greatest value. Contingency theory addresses the concept of contingent conditions, positing that both external and internal factors influence organizational management and may subsequently affect the competencies necessary for competitiveness in dynamic environments (Naseer et al., 2016).

2.2. Conceptual respect

Digital intelligence. According to Na-Nan et al. (2019), DI comprises a comprehensive set of technical, cognitive, and socio-emotional skills that enable an individual to face challenges and adapt to the digital era.

Moral intelligence. According to Al-Adamat et al. (2020), MI refers to a person's moral capacity to integrate intellectual and emotional components into actions according to social norms. In addition, MI is also understood as the ability to process moral information and manage self-regulation.

Digital forensic accounting. According to Kaur et al. (2023), forensic accounting integrates accounting expertise, knowledge, and investigative skills to detect financial crimes to provide evidence to support litigation. Therefore, digital forensic accounting is defined as the application of advances in digital technology to perform forensic accounting activities, including fraud analysis, risk assessment, identification of financial reporting discrepancies, identification of cybercrime, and illegal money transfers.

Cybersecurity performance. Cybersecurity performance management involves the ongoing evaluation of security posture using measures like financial exposure, hence aiding decision-makers in making more informed governance choices. Organizations proficient in cybersecurity management implement processes that regulate the confidentiality, integrity, and availability of information inside their cybersecurity framework. These can assist organizations in attaining cybersecurity performance by enhancing their organizational robustness and resilience against breaches and attacks.

3. Hypothesis development

DI refers to an individual's ability to use digital technology to collect and analyze in-depth data to make recommendations to managers. Accountants possessing advanced digital intelligence can promote and facilitate the implementation of artificial intelligence-based cybersecurity solutions. These technologies can automate threat detection, uncover vulnerabilities, and respond to occurrences in real-time, therefore greatly improving the university's security posture. Accountants can aid in formulating comprehensive cybersecurity strategies and ensuring adherence to pertinent rules. This encompasses routine audits and revisions of security protocols to correspond with emerging threats. Accountants can employ their analytical talents to assess and prioritize risks efficiently. Accountants can use real-time monitoring systems to follow user activity and spot irregularities, facilitating the early discovery and prevention of insider risks. In view of this, the hypotheses guiding this investigation are considered as follows.

Hypothesis 1 (H1). DI significantly and positively affects DFA

Hypothesis 2 (H2). DI significantly and positively affects CYP

A high MI enables individuals to attain a more thorough comprehension and make informed decisions based on their experiences. Consequently, individuals will exhibit greater adaptability to the work environment and possess the capacity to execute assigned duties innovatively while adhering to professional ethical norms. Accountants can promote explicit accountability frameworks for cybersecurity roles and responsibilities, guaranteeing that all individuals comprehend their duties to safeguard sensitive information. By demonstrating ethical conduct, accountants can encourage others within the university community to emphasize ethical issues in their cybersecurity operations. Accountants may promote transparent communication on cybersecurity policies and practices, ensuring that all stakeholders are aware and involved in the process. In view of this, the hypotheses guiding this investigation are considered as follows.

Hypothesis 3 (H3). MI significantly and positively affects DFA

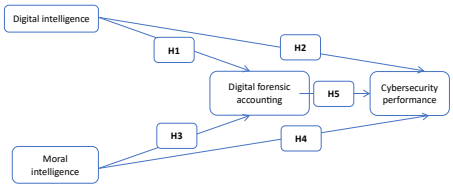
Hypothesis 4 (H4). MI significantly and positively affects CYP

Digital forensics play a pivotal role in navigating the intersection of technology and law. Digital forensics is crucial in investigating and gathering evidence against individuals or organizations that commit crimes in the online environment. With the support of digital technology, forensic accountants can examine financial data in detail to detect discrepancies, irregularities, and fraudulent or erroneous activities. In addition, with the

support of digital technology, forensic accountants will contribute to helping organizations build, maintain, and improve the effectiveness and efficiency of cybersecurity within organization. In view of this, the hypothesis guiding this investigation is considered as follows.

Hypothesis 5 (H5). DFA significantly and positively affects CYP

Figure 1. Conceptual model



4. Research methodology

4.1. Operationalization of the measured variables

This research employed a closed-ended questionnaire. To fulfill the study's objectives, a comprehensive literature analysis was performed to define the research constructs, and many items from each construct were identified to create the preliminary questionnaire. The questionnaire was composed in English and subsequently translated into Vietnamese to facilitate dataset creation and data analysis by multilingual experts, who then performed a reverse translation. The two English questionnaires were subsequently compared to verify the consistency of the survey items. The questionnaire for the study was first evaluated for content and face validity.

Digital intelligence. This investigation determined the DI construct as an elevated amalgamation of four fundamental constructs Data collection and processing capability; Customer service personalization capability; Digital intelligence decision support capability; Sustainable development capability which were inherited from the recommendations of Dong and Wang (2025).

Moral intelligence. This investigation determined the DI construct as an elevated amalgamation of three fundamental constructs Moral sensitivity; Moral commitment; Moral courage which were inherited from the recommendations of Mohammadi et al. (2024).

Digital forensic accounting. This investigation utilized several items that were derived from those proposed by Awodiran et al. (2023) in order to evaluate DFA.

Cybersecurity performance. This investigation determined the DI construct as an elevated amalgamation of five fundamental constructs Cybersecurity capability; Focus on cybersecurity elements; Cyber risk; Cyber resilience; Preparation effort which were inherited from the recommendations of Garcia-Perez et al. (2023).

4.2. Target population and data collection

The accountants affiliated with Vietnamese public universities and public sector organizations were surveyed to ensure the accuracy of the research findings and to reflect a factual scenario. Participants were guaranteed that their involvement and replies would remain entirely anonymous, confidential, and voluntary. The research included non-probability convenience and snowball sampling methods. The recommended sample size ranged from 5:1 to 20:1, with 5 and 20 being the sample size per item. The surveys were disseminated to the respondents from late January 2025 until early April 2025. Following the exclusion of questionnaires plagued by significant flaws, anomalous responses, or inconsistencies, 428 valid questionnaires were ultimately acquired, achieving an effective response rate of 71.33 percent. All informants have a minimum of an undergraduate degree and nine years of experience. The statistical data was analyzed using structural equation modeling with the support of AMOS 28.

5. Results analysis

5.1. Measurement model assessment

Table 1. Results summary of reliability and convergent validity

Constructs and operationalization Factor Loadings		Convergent validity		Construct reliability		Result
		Factor Loadings	AVE	Cronbach's Alpha	Composite Reliability	
Digital intelligence	**DI**					
Data collection and processing capability	DCPC	0.788 - 0.880	0.683	0.864	0.865	Retained
Customer service personalization capability	CSPC	0.801 - 0.870	0.704	0.876	0.877	Retained
Digital intelligence decision support capability	DIDSC	0.716 - 0.909	0.648	0.840	0.846	Retained
Sustainable development capability	SDC	0.731 - 0.852	0.608	0.820	0.822	Retained
Moral intelligence	**MI**					
Moral sensitivity	MS	0.750 - 0.818	0.611	0.822	0.824	Retained
Moral commitment	MOM	0.768 - 0.800	0.602	0.816	0.819	Retained
Moral courage	MOU	0.754 - 0.848	0.630	0.834	0.836	Retained
Digital forensic accounting	**DFA**	0.762 - 0.820	0.623	0.907	0.908	Retained
Cybersecurity performance	**CYP**					
Cybersecurity capability	CAP	0.764 - 0.802	0.621	0.830	0.831	Retained
Focus on cybersecurity elements	FOC	0.773 - 0.902	0.683	0.861	0.866	Retained
Cyber risk	RISK	0.832 - 0.896	0.747	0.845	0.854	Retained
Cyber resilience	RES	0.741 - 0.854	0.623	0.830	0.832	Retained
Preparation effort	PREP	0.717 - 0.865	0.587	0.805	0.810	Retained

The CFA was conducted using the maximum likelihood technique and the support of AMOS 28.0. The Chi-square/df was 1.239 (criteria: ≤ 3), RMSEA was 0.024 (criteria: < 0.08), GFI was 0.911 (criteria: > 0.9), CFI was 0.979 (criteria: > 0.9), TLI was 0.976 (criteria: > 0.9). The reliability of the construct was initially validated using Cronbach's alpha coefficients (Refer Table 1), which ranged from 0.805 to 0.907 across the various constructs. The elevated Cronbach 's alpha values signified a superior degree of internal consistency within each construct, exceeding the commonly recognized threshold of 0.7, hence indicating adequate reliability. Moreover, composite reliability in Table 1, ranging from 0.810 to 0.908, demonstrated comparable assurances of internal consistency, with values far over the threshold of 0.7, so reinforcing the instruments' reliability in evaluating the intended constructs. The factor loadings in Table 1 ranged from 0.716 to 0.909. The average variance extracted (AVE)

values exceeding 0.5 were essential for demonstrating convergent validity. The AVE values varied between 0.587 and 0.747, so demonstrating the convergent validity of the measurement model (Refer Table 1).

The Heterotrait-Monotrait ratio of correlations (HTMT) has been considered as an alternative criterion for identifying issues related to discriminant validity. The optimal cut-off value was supposed to be less than 0.85. The statistical findings clearly show that all values fall below the suggested threshold of 0.85. Therefore, this research attained discriminant validity.

5.2. Structural model assessment

Direct effect. The statistical data revealed that chi-square/df was 1.237 (criteria: ≤ 3), RMSEA was 0.024 (criteria: < 0.08), GFI was 0.904 (criteria: > 0.9), CFI was 0.978 (criteria: > 0.9), TLI was 0.976 (criteria: > 0.9). Table 2 displayed the results of hypothesis testing, confirming all hypotheses. Hypothesis 1 was validated as the DI demonstrated a positive connection with DFA (H1: β=0.344; p=0.000). Hypothesis 2 was validated as the DI demonstrated a positive connection with CYP (H2: β=0.371; p=0.001). Hypothesis 3 was validated as the MI demonstrated a positive connection with DFA (H3: β=0.287; p=0.000). Hypothesis 4 was validated as the MI demonstrated a positive connection with CYP (H4: β=0.448; p=0.000). Hypothesis 5 was validated as the DFA demonstrated a positive connection with CYP (H5: β=0.203; p=0.021). Consequently, H1-H5 received empirical support.

Table 2. Structural coefficients (β) of the hypothesized model

Hypothesis No	Relationship			Standardized	S.E.	C.R.	P	Inference
H1	DI	→	DFA	0.344	0.144	4.027	0.000	Supported
H2	DI	→	CYP	0.371	0.126	3.209	0.001	Supported
H3	MI	→	DFA	0.287	0.121	3.341	0.000	Supported
H4	MI	→	CYP	0.448	0.118	3.428	0.000	Supported
H5	DFA	→	CYP	0.203	0.056	2.308	0.021	Supported

Indirect effect. The mediation investigated was conducted, revealing a substantially and positively indirect effect of DI on CYP via DFA (β= 0.070; p=0.029). The results demonstrated that both direct and indirect paths from DI to CYP were significant and positive through the underlying mechanism of DFA. Additionally, the statistical result also highlighted the substantially and positively indirect effect of MI on CYP via DFA (β= 0.058; p=0.001). The results demonstrated that both direct and indirect paths from MI to CYP were significant and positive through the underlying mechanism of DFA. Thus, DFA was concluded to act as the mediators in the relationship between DI and CYP as well as the relationship between MI and CYP.

6. Concluding remark

Concerns regarding information security in higher education institutions are increasingly emphasized due to their role as repositories of substantial amounts of data, including personal information of students, faculty, staff, as well as data pertaining to academic and financial activities. Consequently, management agencies and institutions must concentrate on several topics to proactively tackle various concerns associated with cybersecurity, including:

Initially, refining the legal framework pertaining to cybersecurity to ensure alignment with the nation's developmental trajectory, current circumstances, and international standards and guidelines.

Secondly, increasing awareness among learners and staff on the detrimental effects of the network environment. Simultaneously, enhance the dissemination of legal regulations pertaining to network security to ensure that learners and employees of the organization promptly comprehend the regulations governing the management, provision, and utilization of information on electronic platforms and social networks, as well as prohibited conduct within the online environment.

Third, collaborating with professional associations to facilitate training courses on professional skills pertinent to DFA, thereby enhancing accountants' knowledge and competencies in executing DFA within the unit. Furthermore, training programs aimed at enhancing DI and MI for accountants must be prioritized to empower them to effectively utilize digital technologies while adhering to professional ethical norms.

Fourth, enhancing the digital infrastructure within the unit to augment its capability to identify cyber threats and emerging phenomena in cyberspace. These technologies enhance network connection systems and facilitate the detection and prevention of increasingly complex and sophisticated threats inside the network environment.

Acknowledgement: *This work was funded by University of Economics Ho Chi Minh City with the Research Topic in University-level at the Grant Number CS-COB-2024-35.*

References:

Al-Adamat, A., Al-Gasawneh, J., & Al-Adamat, O. (2020). The impact of moral intelligence on green purchase intention. Management Science Letters, 10(9), 2063-2070. https://doi.org/10.5267/j.msl.2020.2.005.

Alshurafat, H., Al Shbail, M. O., & Almuiet, M. (2024). Factors affecting the intention to adopt IT forensic accounting tools to detect financial cybercrimes. International Journal of Business Excellence, 33(2), 169-190. https://doi.org/10.1504/IJBEX.2024.139917.

Awodiran, M. A., Ogundele, A. T., Idem, U. J., & Emem O. A. (2023). Digital Forensic Accounting and Cyber Fraud in Nigeria. 2023 International Conference On Cyber Management And Engineering (CyMaEn), 26-27 January 2023, Bangkok, Thailand.

Dong, Y., & Wang, M. (2025). Hotel digital intelligence capability: dimension exploration and scale development. Journal of Hospitality and Tourism Technology, 1-20. https://doi.org/10.1108/JHTT-07-2024-0419.

Garcia-Perez, A., Sallos, M.P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. Journal of Intellectual Capital, 24(2), 465-486. https://doi.org/10.1108/JIC-06-2021-0166.

Kaur, B., Sood, K., & Grima, S. (2023). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. Journal of Financial Regulation and Compliance, 31(1), 60-95. https://doi.org/10.1108/JFRC-02-2022-0015.

Ling-yee, L. (2007). Marketing resources and performance of exhibitor firms in trade shows: A contingent resource perspective. Industrial Marketing Management, 36(3), 360-370. https://doi.org/10.1016/j.indmarman.2005.11.001.

Mohammadi, F., Borzou, S.R., Khazaei, S., Bijani, M., Masoumi, S. Z., & Hosseini, S. K. (2024). Designing and psychometric assessment of the moral intelligence scale for healthcare professionals. Scientific reports, 14, 1-10. https://doi.org/10.1038/s41598-024-55052-2.

Na-Nan, K., Roopleam, T., & Wongsuwan, N. (2019). Validation of a digital intelligence quotient questionnaire for employee of small and medium-sized Thai enterprises using exploratory and confirmatory factor analysis. Kybernetes, 49(5), 1465-1483. https://doi.org/10.1108/k-01-2019-0053.

Naseer, H., Shanks, G., Ahmad, A., & Maynard, S. (2016). Enhancing information security risk management with security analytics: A dynamic capabilities perspective. Australasian conference on information systems, 1-11.

Nazaripour, M., & Zakizadeh, B. (2025). Moral intelligence, emotional intelligence, organizational commitment and job performance of accountants. Accounting Research Journal, 38(1), 19-34. https://doi.org/10.1108/ARJ-01-2024-0034.