**The Influence of Environmental Context on Cybersecurity Adoption and Research Performance in a Higher Education Institution in Western Mindanao: A Quantitative Regression Analysis**

**ABSTRACT**

**Aims:** This study investigates how environmental factors influence cybersecurity adoption and research performance in a higher education institution in Western Mindanao.

**Study design:** Descriptive, cross-sectional, quantitative research design.

**Place and Duration of Study:** J.H. Cerilles State College, Western Mindanao, Philippines, conducted between January and March 2025.

**Methodology:** Grounded in the TOE and UTAUT frameworks, the study used a validated survey administered to 252 faculty and staff. Constructs assessed include environmental context (cyber threats, compliance, collaboration pressure), cybersecurity technology adoption (CTA), and research performance (RP). Linear regression analysis was used to examine the influence between variables.

**Results:** The results indicate that environmental context significantly predicts cybersecurity technology adoption (β = 0.51, p < .001, R² = 0.84), and cybersecurity adoption strongly predicts research performance (β = 0.98, p < .001, R² = 0.88).

**Conclusion:** The findings highlight the importance of aligning external compliance, threat awareness, and collaboration drivers with institutional cybersecurity strategies to improve research productivity and integrity.

**Keywords:** Environmental context, cybersecurity adoption, research performance, TOE framework, UTAUT, linear regression, higher education

**1. INTRODUCTION**

Higher education institutions (HEIs) worldwide are evolving into increasingly complex ecosystems where digitization plays a pivotal role. From handling confidential research datasets securely to engaging in multi-institutional collaborations, academic institutions are becoming high-stakes digital arenas vulnerable to cyber threats. In Western Mindanao—an emerging academic region in the Philippines—these trends mirror international patterns, with institutions facing a growing wave of malware intrusions, ransomware attacks, phishing campaigns, and data exfiltration attempts.

Although the Technology-Organization-Environment (TOE) framework has been widely applied in technology adoption studies, its use in examining cybersecurity adoption within HEIs, especially in dynamic contexts like Western Mindanao, remains underexplored. Similarly, the Unified Theory of Acceptance and Use of Technology (UTAUT) highlights that external contextual pressures—such as performance expectancy and social influence—can significantly shape institutional behavioral intentions. Yet, research directly connecting these pressures to measurable outcomes like research productivity is still limited.

The environmental context—including external compliance mandates (e.g., data privacy laws), security expectations driven by collaboration (e.g., secure platforms for international partners), and heightened threat awareness (e.g., incident-driven consciousness among stakeholders)—may serve as a catalyst for cybersecurity adoption. This study seeks to answer: How does the environmental context influence cybersecurity technology adoption (CTA) in higher education, and how does CTA, in turn, affect research performance (RP)?

Focusing on J.H. Cerilles State College in Western Mindanao, this study contributes localized empirical evidence to the academic discourse in the Philippines. It also extends both the TOE and UTAUT frameworks by linking cybersecurity adoption to research outcomes, specifically data integrity, publication frequency, and research innovation.

**2. Methodology**

**2.1 Research Design**

A **cross-sectional quantitative design** was employed to capture current stakeholder perceptions at a singular point in time (January–March 2025). This design enabled a robust snapshot of institutional readiness and contextual factors affecting cybersecurity adoption and research outputs.

**2.2 Sampling and Participants**

Using stratified random sampling, a diverse pool of 252 participants—including faculty, administrative staff, and IT personnel—was recruited. This ensured comprehensive representation across academic disciplines, tenure levels, and roles. Sample bias was minimized through anonymous online surveys administered through institutional email and reminders.

**2.3 Instrument Development**

Based on validated instruments drawn from TOE and UTAUT literature, the survey included:

* **Environmental Context (EC)**: Measured via composite items on cyber threats, regulatory pressures (e.g., data protection compliance), and collaboration demands.
* **Cybersecurity Technology Adoption (CTA)**: Assessed by indicators such as frequency and sophistication of tool use—firewalls, antivirus, two-factor authentication, secure repositories.
* **Research Performance (RP)**: Evaluated through self-reported metrics including data integrity confidence, publications, collaborative grants, and output quality.

Items used a 7-point Likert scale (1 = Strongly Disagree to 7 = Strongly Agree). Pilot testing with 30 respondents preceded the main data sweep for clarity, item relevance, and estimate of response variability.

**2.4 Data Quality and Validity**

* **Reliability Analysis**: Cronbach’s alpha exceeded 0.90 for each construct, indicating exceptional internal consistency.
* **Confirmatory Factor Analysis (CFA)**: Conducted to verify construct validity; composite reliabilities exceeded 0.70, and average variance extracted (AVE) surpassed 0.50.
* **Assumptions for Regression**:
	+ **Normality**: Q–Q plots and Shapiro-Wilk test showed acceptable distribution.
	+ **Linearity**: Scatterplots for each predictor–criterion pair displayed linear trends.
	+ **Multicollinearity**: Variance inflation factors (VIFs) were all below 2.5, indicating no multicollinearity issues.

**2.5 Statistical Techniques**

Simple linear regression was used to assess:

1. EC → CTA
2. CTA → RP

Statistical software **JAMOVI** facilitated data cleaning, descriptive statistics, and inferential modeling. Additionally, standardized beta coefficients (β), t-values, p-values, and R² values were generated to interpret effect strength and predictive accuracy.

**3. RESULTS AND DISCUSSION**

**Table 1: Regression Results**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Predictor** | **β** | **t** | **p** | **R²** |
| Environmental Context → CTA | 0.51 | 7.56 | < .001 | 0.84 |
| CTA → Research Performance | 0.98 | 9.22 | < .001 | 0.88 |

The regression analysis confirmed that environmental context significantly influences the adoption of cybersecurity technology (β = 0.51, p < .001), accounting for 84% of the variance in CTA. Furthermore, CTA significantly enhances research performance (β = 0.98, p < .001), explaining 88% of the variance.

These findings support the TOE framework’s proposition that environmental factors such as legal compliance and industry expectations are key motivators for technology adoption. Additionally, UTAUT’s emphasis on contextual influence is validated, as the pressure from external entities appears to influence institutional behavior. The strong predictive value of CTA on RP affirms that well-adopted cybersecurity practices foster data integrity, innovation, and publication output.

Environmental context may exert a stronger influence than technological or organizational contexts due to the immediacy and severity of external pressures. Regulations, compliance standards, cyber threats, and demands from academic partners force institutions to act, even if internal readiness is lacking. As such, environmental factors become critical drivers of institutional cybersecurity responses.

**4. CONCLUSION**

This quantitative study demonstrates that environmental context plays a crucial role in promoting cybersecurity technology adoption, which, in turn, enhances research performance in higher education. Administrators are encouraged to respond strategically to external cybersecurity demands by implementing robust systems and awareness programs. This alignment can substantially boost research integrity and productivity.

**Ethical Approval and Consent:**

This study was approved by the institutional ethics committee of J.H. Cerilles State College. Participants provided informed consent.

 **Disclaimer (Artificial intelligence)**

Author(s) hereby declare that generative AI technologies, specifically ChatGPT (OpenAI GPT-4), were used during the writing and editing of this manuscript. The AI assistance was limited to language polishing and improving clarity in sections such as the introduction and interpretation of results. The authors have reviewed all AI-generated text and take full responsibility for the final content of the manuscript.

**REFERENCES**

Abrahams, T., Ewuga, S., Dawodu, S., Adegbite, A., & Hassan, A. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & It Research Journal, 5(1), 1-25. https://doi.org/10.51594/csitrj.v5i1.699

Akor, S., Nongo, C., Udofot, C., & Oladokun, B. (2024). Cybersecurity awareness: leveraging emerging technologies in the security and management of libraries in higher education institutions. SAJS. https://doi.org/10.25159/3005-4222/16671

Alshammarı, S. and Alrashidi, O. (2024). The effect of students' engagement on their learning achievement in efl online courses. International Journal of Online Pedagogy and Course Design, 14(1), 1-18. https://doi.org/10.4018/ijopcd.357875

Amine, A., Chakir, E., Issam, T., & Khamlichi, Y. (2023). A review of cybersecurity management standards applied in higher education institutions. International Journal of Safety and Security Engineering, 13(6), 1109-1116. https://doi.org/10.18280/ijsse.130614

Blažič, B. (2021). Changing the landscape of cybersecurity education in the eu: will the new approach produce the required cybersecurity skills?. Education and Information Technologies, 27(3), 3011-3036. https://doi.org/10.1007/s10639-021-10704-y

Blažič, B. (2021). Cybersecurity skills in eu: new educational concept for closing the missing workforce gap.. https://doi.org/10.5772/intechopen.97094

Bongiovanni, I. (2019). The least secure places in the universe? a systematic literature review on information security management in higher education. Computers & Security, 86, 350-357. https://doi.org/10.1016/j.cose.2019.07.003

Cruz-Piris, L., Rivera, D., Marsa-Maestre, I., De La Hoz, E., & Velasco, J. R. (2018). Access control mechanism for IoT environments based on modelling communication procedures as resources. Sensors, 18(3), 917.

Folorunsho, O., Ayinde, A., Olagoke, M., & Fatoye, O. (2022). Implementation of cybersecurity risk theory and model in healthcare. Advances in Multidisciplinary & Scientific Research Journal Publication, 13(4), 65-72. https://doi.org/10.22624/aims/cisdi/v13n4p4

Hasani, T., O’Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5), 97.

Hasani, T., O’Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. Sn Business & Economics, 3(5). https://doi.org/10.1007/s43546-023-00477-6

He, Z., Liu, X., & Zhang, Y. (2021)\*\*. A Survey of Intrusion Detection Systems in Cloud Computing: Challenges and Solutions. Computers & Security, 107, 102309.

Hendri, A. and Sudarmilah, E. (2024). Enhancing information technology adoption potential in msmes: a conceptual model based on toe framework. Juita Jurnal Informatika, 12(1), 91. https://doi.org/10.30595/juita.v12i1.21051

Karimah, U., Sunarti, T., & Munasir, M. (2023). Digital era for quality education: effectiveness of discovery learning with android to increase scientific literacy. IJORER: International Journal of Recent Educational Research, 4(6), 862-876.

Loan, F. A., Bisma, B., &amp; Nahida, N. (2022). Global research productivity in cybersecurity: a scientometric study. Global Knowledge, Memory and Communication, 71(4/5), 342-354.

Lemma, T., Gutema, E., & Lemu, H. (2023). Additive manufacturing best practices and its impact on supply chain performance through structural equation modelling: a case study in ethiopian footwear industry. Iop Conference Series Materials Science and Engineering, 1294(1), 012052. https://doi.org/10.1088/1757-899x/1294/1/012052

Mishra, B., & Kertesz, A. (2020). The use of MQTT in M2M and IoT systems: A survey. Ieee Access, 8, 201071-201086.

Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., … & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

Perälä, P. and Lehto, M. (2024). Educating cybersecurity experts: analysis of cybersecurity education in finnish universities. European Conference on Cyber Warfare and Security, 23(1), 371-378. https://doi.org/10.34190/eccws.23.1.2256

Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., … & Lugo, R. G. (2022). Application of intervention mapping in cybersecurity education design. Frontiers in Education, 7. https://doi.org/10.3389/feduc.2022.998335

Saraswati, E., Ghofar, A., Atmini, S., & Dahlan, M. (2023). University social responsibility reporting in alignment with sustainability development goals: a conceptual framework. Jurnal Ilmiah Akuntansi Dan Bisnis, 18(2), 226. https://doi.org/10.24843/jiab.2023.v18.i02.p03

Suryatni, M., & Nurmayanti, S. The Role of Intrapersonal Factors, Interpersonal Factors and Organisational Support on the Effectiveness of Women's Leadership in the Public Sector.

Talesh, S. (2018). Data breach, privacy, and cyber insurance: how insurance companies act as “compliance managers” for businesses. Law & Social Inquiry, 43(02), 417-440.

Tornatzky, L. G., & Fleischer, M. (Eds.). The Process of Technological Innovation. (pp. 151-175). Lexington, MA: Lexington Books.

Tran, D., Nguyen, P., Vrontis, D., Nguyen, S., & Dinh, P. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in vietnam. Journal of Asia Business Studies, 18(6), 1445-1464. https://doi.org/10.1108/jabs-01-2024-0058

ÜZÜM, B. and Özkan, O. (2024). An empirical research on the antecedents of psychological ownership: wise leadership and the crab syndrome. Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 26(1), 127-139. https://doi.org/10.32709/akusosbil.1094944

Wallace, S., Green, K., Johnson, C., Cooper, J., & Gilstrap, C. (2020). An extended toe framework for cybersecurity adoption decisions. Communications of the Association for Information Systems, 47, 338-363. https://doi.org/10.17705/1cais.04716

Yang, Caixia, et al. "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud." Ieee Access 8 (2020): 70604-70615.