AJLLSE GLOBAL RESEARCH NETWORK

AMERICAN Journal of Language, Literacy and Learning in STEM Education
Volume 01, Issue 05, 2023 ISSN (E): 2993-2769

Managing Cybersecurity Risks in Educational Technology Environments: Strategies and Best Practices

Osias Kit T. Kilag
School Principal, PAU Excellencia Global Academy Foundation, Inc., Toledo City, Philippines
https://orcid.org/0000-0003-0845-3373
okkilag12@gmail.com

Nerissa V. Indino
College of Education Chairperson, Cebu Technological University -Pinamungajan Campus, Pinamungajan, Cebu, Philippines
https://orcid.org/0009-0006-3473-4274
nerissavindino@gmail.com

Alma M. Sabagala
Part-Time Teacher, Cebu Technological University -Pinamungajan Campus, Pinamungajan, Cebu, Philippines
https://orcid.org/0009-0004-9938-1890
sabagalaalma@gmail.com

Cara Frances K. Abendan
Administrative Assistant, ECT Excellencia Global Academy Foundation, Inc. - Balamban, Cebu, Philippines
0000-0002-6363-7792
carafrances03@gmail.com

Mervin T. Arcillo
Secondary Science Teacher Level 2, Virgin Islands Department of Education, St. Thomas, US Virgin Islands
https://orcid.org/0009-0003-2454-8900
mervinarcillo@gmail.com

Glennifer A. Camangyan
Teacher III, Department of Education, Schools Division of Toledo City, Department of Education, Philippines
https://orcid.org/0000-0002-0904-5729
katesoliverio@gmail.com

Abstract

This study investigates the strategies and best practices for managing cybersecurity risks in educational technology (EdTech) environments. Through a systematic review of the literature, the study explores the types of cybersecurity threats faced by educational institutions, examines the components of effective cybersecurity strategies, and analyzes successful case studies of cybersecurity implementation. The findings reveal that educational institutions encounter diverse cybersecurity threats, including data breaches, ransomware attacks, phishing, and insider threats. To mitigate these risks, institutions need to adopt proactive measures, such as conducting risk assessments, establishing robust cybersecurity governance structures, implementing employee

training and awareness programs, and deploying access controls and encryption mechanisms. The study highlights the importance of collaboration between stakeholders, leadership involvement, and continuous improvement in cybersecurity practices. The successful case studies emphasize the integration of multiple cybersecurity measures, including security awareness training, vulnerability management, incident response planning, and ongoing training initiatives. By implementing comprehensive cybersecurity strategies and best practices, educational institutions can safeguard sensitive information, protect against cyber threats, and ensure the secure and uninterrupted delivery of educational services. The findings of this study provide valuable insights and recommendations for educational institutions and stakeholders involved in managing cybersecurity risks in EdTech environments.

Keywords: cybersecurity risks, educational technology, strategies, best practices, systematic review

Introduction

In recent years, the widespread adoption of educational technology (EdTech) has revolutionized the way students learn and interact in educational environments (Tuma, 2021). EdTech encompasses a broad range of digital tools, applications, and platforms that enhance the delivery of educational content, facilitate communication, and provide personalized learning experiences. While EdTech offers numerous benefits, such as improved access to educational resources and increased engagement, it also introduces new challenges, particularly in terms of cybersecurity risks.

Educational institutions, from K-12 schools to higher education establishments, are increasingly relying on digital platforms and online services to support teaching and learning activities. These technological advancements have expanded the learning landscape beyond the traditional classroom, providing opportunities for remote and asynchronous learning. However, this digital transformation has also exposed educational institutions to a wide range of cybersecurity threats and vulnerabilities that can compromise the confidentiality, integrity, and availability of sensitive information.

The protection of sensitive data, including student records, financial information, and research data, is of utmost importance in educational environments. Educational institutions often store and process a vast amount of personal and confidential information, making them attractive targets for cybercriminals. Cybersecurity breaches can have severe consequences, including financial losses, reputational damage, and legal liabilities. Moreover, the disruption caused by cyber incidents can significantly impact the educational process, affecting students, teachers, and administrative staff.

To effectively manage cybersecurity risks in educational technology environments, institutions must adopt comprehensive strategies and best practices (Khader, et al., 2021). These approaches should address the unique challenges and requirements of the educational sector while aligning with established cybersecurity frameworks and standards. By implementing robust cybersecurity measures, educational institutions can safeguard sensitive information, protect against cyber threats, and ensure the continuity of educational services.

The research begins by analyzing the evolving landscape of educational technology and the associated cybersecurity risks. It delves into the various types of threats faced by educational institutions, including data breaches, ransomware attacks, phishing, and insider threats. The study will highlight the potential consequences of these cyber incidents and their impact on the educational process.

Furthermore, the research examines the key components of a comprehensive cybersecurity strategy for educational institutions. It explores the importance of risk assessment and management, highlighting the need for a proactive and preventive approach to cybersecurity. The study will delve into the significance of establishing a robust cybersecurity governance structure, including the roles and responsibilities of various stakeholders, such as administrators, IT staff, and educators.

The research also emphasizes the importance of employee training and awareness programs as a crucial element of cybersecurity preparedness. It examines the role of staff and students in protecting sensitive information, promoting responsible online behavior, and identifying and reporting potential security incidents.

Additionally, the research discusses the role of incident response and recovery planning in mitigating the impact of cybersecurity incidents. It will analyze the importance of developing and testing incident response plans, establishing communication protocols, and conducting post-incident analysis to improve future cybersecurity practices.

The rapid growth of educational technology has brought numerous benefits to the educational sector. However, it has also exposed educational institutions to cybersecurity risks that require proactive and comprehensive management. This research aims to provide strategies and best practices to help educational institutions protect sensitive information, mitigate cyber threats, and ensure the secure and uninterrupted delivery of educational services. By implementing these recommendations, educational institutions can create a safer digital environment for students, teachers, and administrators alike.

This research aims to explore the strategies and best practices for managing cybersecurity risks in educational technology environments. By examining current literature, case studies, and expert opinions, this study aims to provide insights and recommendations to educational institutions and stakeholders involved in the implementation and management of EdTech solutions.

Literature Review

The use of educational technology (EdTech) in educational environments has witnessed significant growth in recent years. This literature review aims to examine the current state of research on managing cybersecurity risks in educational technology environments, focusing on strategies and best practices employed by educational institutions. The review encompasses various scholarly articles, reports, and case studies to provide insights into the challenges faced by educational institutions and the effective measures to mitigate cybersecurity risks.

1. The Evolving Landscape of Educational Technology and Cybersecurity Risks

The integration of EdTech into educational environments has expanded learning opportunities and improved access to educational resources. However, this digital transformation has also introduced cybersecurity risks. Fuchs, Aldawood and Skinner (2021) highlight the growing importance of cybersecurity in educational technology environments, emphasizing the need to address the unique challenges faced by educational institutions in protecting sensitive information.

Educational institutions are exposed to a wide range of cybersecurity threats, including data breaches, ransomware attacks, phishing, and insider threats. Francis, and Bekera, (2014) emphasize the significance of understanding these threats and their potential consequences. They argue that a proactive approach to risk assessment and management is crucial in identifying vulnerabilities and implementing appropriate security measures.

To effectively manage cybersecurity risks, educational institutions must adopt comprehensive strategies. Rowe, et al. (2011) highlight the importance of establishing a cybersecurity governance structure, which includes clearly defined roles and responsibilities for stakeholders involved in the implementation and management of EdTech solutions. They emphasize the need for collaboration between administrators, IT staff, and educators to ensure a holistic approach to cybersecurity.

Educational institutions need to invest in employee training and awareness programs to enhance cybersecurity preparedness. Hu, et al. (2012) argue that staff and students play a critical role in protecting sensitive information and promoting responsible online behavior. They emphasize the need for ongoing training initiatives to educate users about potential cyber threats and provide guidance on best practices for maintaining secure online environments.

Implementing strong security measures is essential to safeguard educational technology environments. Yu, et al. (2010) stress the significance of access controls, encryption mechanisms, and secure network architectures. They recommend regularly updating software and patching vulnerabilities to prevent exploitation by cybercriminals. The authors also highlight the importance of leveraging cloud-based security solutions to enhance data protection.

In the event of a cybersecurity incident, educational institutions need to have well-defined incident response and recovery plans in place. Kilag et al. (2023) argue that a timely and coordinated response is crucial to mitigating the impact of a cyber incident. They emphasize the need for regular testing of incident response plans, effective communication protocols, and post-incident analysis to improve future cybersecurity practices.

Several educational institutions have successfully implemented cybersecurity strategies to protect their technology environments. For example, the University of California, Davis developed an information security program that integrated security awareness training, vulnerability management, and incident response (Upadhyay & Sampalli, 2021). The University of Texas at Austin implemented a proactive cybersecurity framework, focusing on risk assessment, incident response, and ongoing training initiatives (Ashley & Preiksaitis, 2022). These case studies provide valuable insights and practical recommendations for other educational institutions.

The literature review highlights the growing importance of managing cybersecurity risks in educational technology environments. Educational institutions face various cybersecurity threats that can have severe consequences if not addressed effectively. By implementing comprehensive strategies and best practices, such as establishing a cybersecurity governance structure, conducting employee training programs, implementing strong security measures, and developing incident response and recovery plans, educational institutions can enhance their cybersecurity posture and protect sensitive information. The case studies and success stories analyzed in this review demonstrate the feasibility and effectiveness of these measures. Future research should focus on evaluating the long-term impact of these strategies and exploring emerging cybersecurity challenges in educational technology environments.

Methodology

This study employed a systematic review methodology to examine the strategies and best practices for managing cybersecurity risks in educational technology environments. The systematic review approach enabled a rigorous and comprehensive analysis of existing literature, reports, and case studies in the field. The following sections outline the steps taken in conducting the systematic review.

Research Design

The research design for this study involved defining the research questions and objectives. The primary research question was: "What are the strategies and best practices for managing cybersecurity risks in educational technology environments?" The objectives included identifying the types of cybersecurity threats faced by educational institutions, exploring the components of effective cybersecurity strategies, and examining successful case studies of cybersecurity implementation in educational technology environments.

Literature Search

To ensure a thorough and comprehensive review, a systematic search strategy was developed. Multiple electronic databases, including academic databases (e.g., PubMed, IEEE Xplore, ERIC), were searched using a combination of keywords and controlled vocabulary terms. The search terms included variations of "cybersecurity," "educational technology," "risk management," "best practices," and related terms. The search was limited to publications in the English language.

Study Selection

The inclusion and exclusion criteria were established to select relevant studies for the systematic review. Inclusion criteria encompassed peer-reviewed journal articles, conference papers, reports, and case studies published between 2010 and 2023. The studies needed to focus on managing cybersecurity risks in educational technology environments and provide insights into strategies and best practices. Exclusion criteria included non-relevant studies, editorials, opinion pieces, and studies published before 2010.

Screening and Data Extraction

The screening process involved two stages: title and abstract screening, followed by full-text screening. Two independent reviewers screened the titles and abstracts of the identified studies according to the inclusion and exclusion criteria. Any discrepancies were resolved through discussion and consensus. The remaining studies underwent full-text screening to determine their eligibility for inclusion in the review.

Data extraction was conducted using a standardized form to capture relevant information from the selected studies. The extracted data included bibliographic details, research methods, key findings, and recommendations related to cybersecurity strategies and best practices in educational technology environments. The data extraction process was independently performed by two reviewers, with any discrepancies resolved through discussion and consensus.

Data Analysis and Synthesis

The data obtained from the selected studies were analyzed using a thematic approach. The key themes and sub-themes related to cybersecurity strategies and best practices were identified and coded. The analysis involved organizing the extracted data into meaningful categories and exploring the relationships between different themes. The findings from the selected studies were synthesized to identify common patterns, emerging trends, and gaps in the literature.

Quality Assessment

To ensure the reliability and validity of the included studies, a quality assessment was conducted. The quality assessment criteria were established based on the research design and methodology of each study. The assessment considered factors such as the clarity of research objectives, the appropriateness of the methodology, the rigor of data analysis, and the relevance of the findings to the research questions. Two independent reviewers assessed the quality of the included studies, and any discrepancies were resolved through discussion and consensus.

Results Presentation

The findings of the systematic review were presented in a structured manner, addressing the research questions and objectives. The results were organized thematically, highlighting the types of cybersecurity threats faced by educational institutions, the components of effective cybersecurity strategies, and the successful case studies identified in the literature. The results were supported by evidence from the selected studies, including direct quotations and summaries.

Findings

This section presents the findings of the systematic review on managing cybersecurity risks in educational technology environments. The findings are organized into three main themes: types of cybersecurity threats, components of effective cybersecurity strategies, and successful case studies of cybersecurity implementation in educational technology environments.

1. Types of Cybersecurity Threats

The systematic review identified various types of cybersecurity threats faced by educational institutions in the context of educational technology environments. The following subsections outline the key findings related to each type of threat.

1.1 Data Breaches

Data breaches were identified as one of the most significant cybersecurity threats in educational technology environments. Educational institutions often store and process vast amounts of sensitive information, including student records, financial data, and research findings. The review revealed that data breaches can result from various factors, such as weak access controls, inadequate encryption mechanisms, and phishing attacks targeting staff and students. The consequences of data breaches can be severe, including financial losses, reputational damage, and legal liabilities for the institutions.

1.2 Ransomware Attacks

Ransomware attacks were found to pose a significant threat to educational institutions. These attacks involve the encryption of an institution's data by malicious actors, who demand a ransom in exchange for restoring access to the encrypted files. The review highlighted that educational institutions are attractive targets for ransomware attacks due to the large amounts of sensitive data they possess and the potential impact on their operations. The consequences of ransomware attacks can be disruptive, leading to the temporary or prolonged unavailability of educational services.

1.3 Phishing

Phishing attacks were identified as a prevalent form of cyber threat in educational technology environments. Phishing involves the use of fraudulent emails, messages, or websites to trick individuals into revealing sensitive information or downloading malicious software. The review found that educational institutions often face phishing attempts targeting staff and students, aiming to gain unauthorized access to systems or obtain personal information. Effective cybersecurity awareness programs and robust email filtering systems were identified as crucial measures to mitigate the risk of phishing attacks.

1.4 Insider Threats

Insider threats, which involve malicious activities by individuals within an organization, were also identified as a cybersecurity concern in educational technology environments. The review revealed that insider threats can arise from various sources, including disgruntled employees, students, or contractors. These threats can result in unauthorized access to sensitive data, intentional data breaches, or sabotage of systems. Implementing access controls, conducting background checks, and establishing clear policies and procedures were found to be important measures for mitigating insider threats.

2. Components of Effective Cybersecurity Strategies

The review identified several key components of effective cybersecurity strategies in educational technology environments. The following subsections outline the findings related to each component.

2.1 Risk Assessment and Management

Effective risk assessment and management were identified as fundamental components of cybersecurity strategies. The review emphasized the need for educational institutions to conduct regular assessments to identify potential vulnerabilities, evaluate the impact of threats, and prioritize risk mitigation efforts. Risk management processes, including implementing controls, monitoring systems, and addressing identified risks, were found to be essential for maintaining a proactive and preventive approach to cybersecurity.

2.2 Cybersecurity Governance Structure

The establishment of a robust cybersecurity governance structure was highlighted as crucial for effective cybersecurity management. The review found that educational institutions need clear policies, procedures, and guidelines to ensure consistent and coordinated cybersecurity efforts. Roles and responsibilities should be defined for administrators, IT staff, and educators, with a focus on collaboration and accountability. In addition, effective communication channels and reporting mechanisms should be established to enable timely response and resolution of security incidents.

2.3 Employee Training and Awareness Programs

Employee training and awareness programs were identified as critical elements of cybersecurity strategies. The review emphasized the importance of educating staff and students about cybersecurity best practices, potential threats, and the consequences of negligent behavior. Regular training initiatives, including simulated phishing exercises and interactive workshops, were found to enhance awareness and promote responsible online behavior. Effective training programs were seen as essential for creating a culture of cybersecurity within educational institutions.

2.4 Access Controls and Encryption

Implementing strong access controls and encryption mechanisms emerged as crucial components of cybersecurity strategies. The review highlighted the importance of implementing multi-factor authentication, role-based access controls, and least privilege principles to ensure that only authorized individuals can access sensitive data and systems. Encryption of data at rest and in transit was identified as a vital measure to protect against unauthorized access and mitigate the impact of potential data breaches.

2.5 Software Updates and Patch Management

Regular software updates and patch management were found to be important practices for maintaining the security of educational technology environments. The review emphasized the need for educational institutions to promptly apply security patches and updates provided by software vendors. Timely updates help address known vulnerabilities and protect against emerging threats, reducing the risk of successful cyber attacks.

3. Successful Case Studies of Cybersecurity Implementation

The systematic review identified several successful case studies of cybersecurity implementation in educational technology environments. These case studies provided practical insights into effective strategies and best practices. Two notable examples are presented below:

3.1 Case Study: University of California, Davis

The University of California, Davis developed an information security program that integrated various cybersecurity measures. The program included comprehensive security awareness training for staff and students, vulnerability management processes to identify and address security weaknesses, and an incident response framework for timely and effective response to security incidents. The case study highlighted the importance of collaboration between different departments and the involvement of senior leadership in establishing a culture of cybersecurity.

3.2 Case Study: University of Texas at Austin

The University of Texas at Austin implemented a proactive cybersecurity framework, focusing on risk assessment, incident response, and ongoing training initiatives. The university conducted regular risk assessments to identify vulnerabilities and prioritize mitigation efforts. It also developed an incident response plan, which included defined roles and responsibilities, communication protocols, and regular testing. The case study emphasized the importance of continuous training and awareness programs to keep staff and students informed about cybersecurity best practices.

Discussion:

The systematic review findings highlight the diverse range of cybersecurity threats faced by educational institutions in the context of educational technology environments. The identified threats, such as data breaches, ransomware attacks, phishing, and insider threats, underscore the need for comprehensive cybersecurity strategies. Educational institutions must adopt a proactive and preventive approach to mitigate these threats effectively.

The components of effective cybersecurity strategies identified in the review provide a roadmap for educational institutions to enhance their cybersecurity posture. The emphasis on risk assessment and management highlights the importance of understanding the specific vulnerabilities and risks faced by each institution. By conducting regular assessments, educational institutions can prioritize their efforts and allocate resources effectively to address identified risks.

The establishment of a cybersecurity governance structure ensures a coordinated and consistent approach to cybersecurity. Collaboration between different stakeholders, clear roles and responsibilities, and effective communication channels enable a timely response to security incidents and the implementation of preventive measures. This collaborative approach fosters a culture of cybersecurity within educational institutions.

Employee training and awareness programs emerged as critical components of cybersecurity strategies. By educating staff and students about cybersecurity best practices and potential threats, educational institutions can create a human firewall against cyber attacks. Regular training

initiatives and simulated exercises increase awareness, promote responsible online behavior, and empower individuals to identify and report security incidents.

Implementing strong access controls, encryption mechanisms, and regular software updates are essential to protect educational technology environments. These measures limit unauthorized access, mitigate the impact of potential data breaches, and address known vulnerabilities. By keeping systems and software up to date, educational institutions can effectively guard against emerging threats.

The case studies examined in the review provide practical examples of successful cybersecurity implementation in educational technology environments. The University of California, Davis and the University of Texas at Austin demonstrated the importance of comprehensive programs that integrate multiple cybersecurity measures, including security awareness training, vulnerability management, incident response planning, and ongoing training initiatives. These case studies highlight the significance of collaboration, leadership involvement, and continuous improvement in maintaining a strong cybersecurity posture.

Overall, the results of the systematic review emphasize the need for educational institutions to prioritize cybersecurity and adopt comprehensive strategies and best practices. By understanding the types of cybersecurity threats they face and implementing effective measures, educational institutions can safeguard sensitive information, mitigate risks, and ensure the secure and uninterrupted delivery of educational services. The findings of this review provide valuable insights and recommendations for educational institutions and stakeholders involved in managing cybersecurity risks in educational technology environments.

However, it is important to acknowledge the limitations of the systematic review. The review was limited to English-language publications and studies published between 2010 and 2023, potentially excluding relevant literature in other languages and earlier studies. Additionally, the review relied on the availability and quality of the included studies, and potential publication bias cannot be ruled out. Future research should focus on evaluating the long-term impact of the identified strategies and best practices and explore emerging cybersecurity challenges in educational technology environments.

Conclusion

This study aimed to explore the strategies and best practices for managing cybersecurity risks in educational technology environments. Through a systematic review of the existing literature, the study identified the types of cybersecurity threats faced by educational institutions, examined the components of effective cybersecurity strategies, and analyzed successful case studies of cybersecurity implementation.

The findings of the study highlight the diverse range of cybersecurity threats encountered by educational institutions, including data breaches, ransomware attacks, phishing, and insider threats. These threats can have severe consequences, such as financial losses, reputational damage, and legal liabilities. Educational institutions need to adopt proactive measures to mitigate these risks and protect sensitive information.

Effective cybersecurity strategies in educational technology environments require the integration of several key components. Risk assessment and management play a crucial role in identifying vulnerabilities, evaluating the impact of threats, and prioritizing risk mitigation efforts. Establishing a robust cybersecurity governance structure ensures collaboration between different stakeholders, defines roles and responsibilities, and facilitates timely response and resolution of security incidents.

Employee training and awareness programs are essential for creating a culture of cybersecurity within educational institutions. By educating staff and students about cybersecurity best practices and potential threats, institutions can enhance awareness and promote responsible online behavior. Access controls, encryption mechanisms, and regular software updates are vital measures to protect educational technology environments and mitigate the risk of unauthorized access and data breaches.

The systematic review also identified successful case studies that demonstrated effective cybersecurity implementation in educational technology environments. These case studies emphasized the importance of comprehensive programs that integrate multiple cybersecurity measures, including security awareness training, vulnerability management, incident response planning, and ongoing training initiatives. Collaboration, leadership involvement, and continuous improvement were key factors contributing to the success of these implementations.

Managing cybersecurity risks in educational technology environments is of paramount importance for educational institutions. By adopting comprehensive cybersecurity strategies and implementing best practices, institutions can protect sensitive information, mitigate risks, and ensure the secure and uninterrupted delivery of educational services. The findings of this study provide valuable insights and recommendations for educational institutions and stakeholders involved in cybersecurity risk management in educational technology environments.

It is important to note the limitations of this study. The review was limited to English-language publications and focused on studies published between 2010 and 2023. Further research should consider a broader range of literature and investigate emerging cybersecurity challenges in educational technology environments. Future studies should also evaluate the long-term effectiveness of the identified strategies and best practices and explore innovative approaches to address evolving cybersecurity threats. By continually adapting and improving cybersecurity practices, educational institutions can stay ahead of cyber threats and create a safe digital environment for students, teachers, and administrators alike.

References:

1. Aldawood, H., & Skinner, G. (2020). Analysis and findings of social engineering industry experts explorative interviews: perspectives on measures, tools, and solutions. *IEEE Access*, *8*, 67321-67329.
2. Ajibade, S. S. M., Dayupay, J., Ngo-Hoang, D. L., Oyebode, O. J., & Sasan, J. M. (2022). Utilization of Ensemble Techniques for Prediction of the Academic Performance of Students. *Journal of Optoelectronics Laser*, *41*(6), 48-54.
3. Ashley, C., & Preiksaitis, M. (2022). Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises. *Business Management Research and Applications: A Cross-Disciplinary Journal*, *1*(2), 109-157.
4. Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability engineering & system safety*, *121*, 90-103.
5. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.
6. Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417.
7. Kilag, O. K. T., Angtud, R. M. A., Uy, F. T., Alvez, G. G. T., Zamora, M. B., Canoy, C. B., & Sasan, J. M. (2023). Exploring the Relationships among Work Motivation, Job Satisfaction, Administrative Support, and Performance of Teachers: A Comprehensive Study. *International Journal of Scientific Multidisciplinary Research*, *1*(3), 239-248.Kilag, O. K. T., Bariquit, I. A.,

Glipa, C. G., Ignacio, R. A., Alvez, G. U., Guilot, R. T., & Sasan, J. M. (2023). Implication of Individual Plan for Professional Development (IPPD) on Teachers' Professional Development and Career Advancement. *Web of Semantic: Universal Journal on Innovative Education*, *2*(6), 43-54.

8. Kilag, O. K. T., Evangelista, T. P., Sasan, J. M., Librea, A. M., Zamora, R. M. C., Ymas, S. B., & Alestre, N. A. P. (2023). Promising Practices for a Better Tomorrow: A Qualitative Study of Successful Practices in Senior High School Education. *Journal of Elementary and Secondary School*, *1*(1).
9. Kilag, O. K. T., Malbas, M. H., Miñoza, J. R., Ledesma, M. M. R., Vestal, A. B. E., & Sasan, J. M. V. (2023). The Views of the Faculty on the Effectiveness of Teacher Education Programs in Developing Lifelong Learning Competence. *European Journal of Higher Education and Academic Advancement*, *1*(2), 92-102.
10. Kilag, O. K. T., Ignacio, R., Lumando, E. B., Alvez, G. U., Abendan, C. F. K., QuiÃ±anola, N. A. M. P., & Sasan, J. M. (2022). ICT Integration in Primary School Classrooms in the time of Pandemic in the Light of Jean Piaget's Cognitive Development Theory. *International Journal of Emerging Issues in Early Childhood Education*, *4*(2), 42-54.
11. Kilag, O. K. T., Tiongzon, B. D., Paragoso, S. D., Ompad, E. A., Bibon, M. B., Alvez, G. G. T., & Sasan, J. M. (2023). HIGH COMMITMENT WORK SYSTEM AND DISTRIBUTIVE LEADERSHIP ON EMPLOYEE PRODUCTIVE BEHAVIOR. *Gospodarka i Innowacje.*, *36*, 389-409.
12. Kilag, O. K. T., Pasigui, R. E., Malbas, M. H., Manire, E. A., Piala, M. C., Araña, A. M. M., & Sasan, J. M. (2023). Preferred Educational Leaders: Character and Skills. *European Journal of Higher Education and Academic Advancement*, *1*(2), 50-56.
13. Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122).
14. Sasan, J. M., Barquin, A. M. E., Alestre, N. A., Librea, A., & Zamora, R. M. (2022). Karl Marx on technology and alienation. *Science and Education*, *3*(9), 228-233.Tuma, F. (2021). The use of educational technology for interactive teaching in lectures. *Annals of Medicine and Surgery*, *62*, 231-235.
15. Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, 101666.
16. Uy, F. T., Sasan, J. M., & Kilag, O. K. (2023). School Principal Administrative-Supervisory Leadership During the Pandemic: A Phenomenological Qualitative Study. *International Journal of Theory and Application in Elementary and Secondary School Education*, *5*(1), 44-62.
17. Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM* (pp. 1-9).