SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Navigating the Digital Frontier: A Review of Cybersecurity in Pangasinan

Wenna Lyn D. Honrado[1]
Pangasinan State University – Asingan Campus

Article Info:
Received: ***10 June 2024;*** *Revised:* ***05 Nov 2024;*** *Accepted:* ***01 Dec 2024;*** *Available Online:* ***15 Jan 2025***

Abstract *– The rapid digital transformation across the Philippines has brought forth unprecedented economic and social opportunities, alongside a burgeoning landscape of cyber threats. This review article synthesizes the current state of cybersecurity in the province of Pangasinan, a significant economic and educational hub in the Ilocos Region. While national-level studies depict a rising tide of cybercrime, including online scams, identity theft, and phishing, a focused scholarly examination of the cybersecurity posture of Pangasinan remains nascent. This paper, following an IMRAD (Introduction, Methodology, Results and Discussion, and Conclusion) structure, conducts a thematic literature review of existing research to map the prevailing cybersecurity trends, challenges, and opportunities within the province. The analysis is predicated on research articles pertaining to cybersecurity, cybercrime, digital literacy, and ICT infrastructure, with a deliberate exclusion of non-academic sources. The findings are thematically organized, exploring cybersecurity in local industries, the pivotal role of academic institutions, the foundational importance of digital literacy among its populace, and the overarching influence of the national cyber threat landscape. This review identifies a critical need for localized cybersecurity strategies that address the specific socio-economic and infrastructural realities of Pangasinan. Key challenges include enhancing the digital literacy of local government officials and the general public, fortifying the cyber defenses of small and medium-sized enterprises (SMEs) which form the backbone of the provincial economy, and fostering a culture of cybersecurity awareness. Recommendations underscore the necessity for collaborative initiatives between local government units, academia, and the private sector to develop targeted training programs, establish a provincial cybersecurity task force, and promote research into the unique cyber risks faced by communities in Pangasinan.* .

Keywords *– Cybersecurity, Pangasinan, literature review, thematic analysis, digital literacy, cybercrime, ICT infrastructure*

INTRODUCTION

The 21st century is defined by an inexorable shift towards digitalization, a paradigm that has profoundly reshaped economies, governance, and societal interactions. In the Philippines, this digital wave has been particularly pronounced, with a burgeoning digital economy and one of the most active social media populations globally. However, this increased connectivity has concurrently exposed individuals, businesses, and government entities to a myriad of cybersecurity threats. The national discourse on cybersecurity is dominated by alarming statistics on cybercrime, including a significant rise in online scams, phishing attacks, and data breaches, compelling the national government to bolster its cyber defense framework through initiatives like the National Cybersecurity Plan (The Asia Foundation, 2022).

While the national perspective provides a crucial backdrop, the nuances of cybersecurity challenges and preparedness at the local level, particularly in provinces like Pangasinan, are often overlooked in scholarly literature. Pangasinan, a major province in the Ilocos Region, is characterized by a diverse economy encompassing agriculture, aquaculture, tourism, and a growing services sector. It is also home to numerous higher education institutions, making it a significant educational center in Northern Luzon. As the province embraces digital technologies for commerce, education, and public service delivery, its vulnerability to cyber threats commensurately increases. Understanding the specific cybersecurity landscape of

Pangasinan is therefore not just an academic exercise but a critical component of ensuring its sustainable and secure development in the digital age.

This review article aims to synthesize the existing body of scholarly research to provide a comprehensive overview of cybersecurity in Pangasinan. By focusing exclusively on research articles, this paper seeks to build a foundational understanding based on empirical evidence and academic inquiry. The subsequent sections will follow the IMRAD format, beginning with a methodology that outlines the literature review process, followed by a thematic analysis of the results and a discussion of the latest cybersecurity trends identifiable from the literature. The article will conclude with a summary of the findings and provide actionable recommendations for enhancing the cybersecurity posture of Pangasinan.

Objectives Of The Study

The objective of this study is to conduct a comprehensive literature review to identify and analyze the current trends, challenges, and opportunities in cybersecurity within the province of Pangasinan. To achieve this, a systematic literature review methodology was employed. This approach was chosen for its ability to synthesize existing research in a structured and transparent manner, providing a robust foundation for understanding the state of cybersecurity in the specified locality.

Materials and Methods

The research process involved a multi-stage approach to the identification, selection, and analysis of relevant scholarly articles. The primary sources for this review were academic databases and search engines, including Google Scholar, ResearchGate, and institutional repositories of Philippine universities. The search strategy utilized a combination of keywords, including "cybersecurity Pangasinan," "cybercrime Pangasinan," "digital literacy Pangasinan," "ICT Pangasinan research," "cybersecurity challenges Philippines," and "cybercrime trends Philippines." The search was limited to research articles, including journal papers, conference proceedings, and academic theses and dissertations, to ensure the scholarly rigor of the reviewed literature. News articles, websites, and other non-academic publications were explicitly excluded from the analysis.

The selection of articles was guided by their direct or indirect relevance to the cybersecurity landscape of Pangasinan. Given the limited number of studies focusing exclusively on the province, the inclusion criteria were broadened to encompass research on digital literacy, ICT infrastructure, and local industry practices within Pangasinan that have significant cybersecurity implications. Additionally, national-level research on cybersecurity trends and challenges in the Philippines was included to provide a broader context for the situation in Pangasinan.

The core of the methodology is a thematic analysis of the selected literature. This involved a careful reading and re-reading of the articles to identify recurring themes, patterns, and concepts related to cybersecurity. The identified themes were then categorized and organized to form the structure of the Results and Discussion section. This thematic approach allows for a coherent synthesis of findings from disparate studies, enabling a holistic understanding of the multifaceted nature of cybersecurity in Pangasinan. By structuring the analysis around key themes, this review aims to present a clear and insightful narrative of the prevailing cybersecurity landscape in the province.

Results and Discussion

The thematic analysis of the collected research articles reveals several key trends and challenges that define the current state of cybersecurity in Pangasinan. While a singular, comprehensive study on the province's overall cybersecurity posture is absent from the current body of literature, a composite picture can be constructed from research focusing on specific sectors, demographic groups, and the broader national context. The following themes emerged as central to understanding cybersecurity in Pangasinan: the digital literacy of its citizens and officials as a critical vulnerability, the cybersecurity readiness of local industries, the role and challenges of academic institutions, and the overarching shadow of the national cybercrime landscape.

Theme 1: Digital Literacy as a Foundational Cybersecurity Challenge

A recurrent theme in the literature related to Pangasinan is the varying and often insufficient levels of digital literacy among different segments of its population. This is a critical concern, as low digital literacy is a direct precursor to heightened vulnerability to a wide array of cyber threats, including phishing, social engineering, and the proliferation of disinformation.

A study on the digital literacy of elected barangay officials in Agno, Pangasinan, revealed that while there is access to digital devices, a significant portion of these grassroots leaders exhibit only an intermediate level of digital literacy (Carpio, 2020). The research highlighted a "fear in using computer and digital gadgets" and a perception that "personal knowledge or experience is still insufficient" (Carpio, 2020, p. 9). This finding is particularly alarming as barangay officials are at the forefront of community governance and are increasingly expected to utilize digital platforms for communication and service delivery. Their lack of advanced digital skills and confidence can impede the secure implementation of e-governance initiatives and makes them susceptible to targeted cyberattacks aimed at gaining access to local government data.

Similarly, research conducted at Pangasinan State University (PSU) on the challenges of online learning pointed to issues with "technological literacy and competency" among students (Cabansag & Ventayen, 2021). While a different demographic, this highlights a broader trend where even the digitally native younger generation may lack the critical digital literacy skills necessary to navigate the online world safely. Their proficiency in using social media and entertainment applications does not always translate into an understanding of cybersecurity best practices, making them vulnerable to online scams, cyberbullying, and identity theft. Further research at PSU corroborated these challenges, particularly in the context of online language and literature learning (Casimiro & Orlanda-Ventayen, 2024).

The implications of these findings for Pangasinan's overall cybersecurity are profound. A populace with inadequate digital literacy is more likely to fall victim to common cyber threats, leading to individual financial losses, emotional distress, and a general erosion of trust in digital technologies. From a community perspective, it creates a fertile ground for cybercriminals and can undermine the effectiveness of digital transformation efforts in the province.

Theme 2: Cybersecurity Preparedness in Local Industries

The economic landscape of Pangasinan is diverse, with a significant contribution from small and medium-sized enterprises (SMEs) in sectors such as tourism, retail, and food processing. The cybersecurity preparedness of these local industries is a crucial factor in the province's economic resilience. However, research in this area, while limited, suggests a developing but not yet mature cybersecurity posture.

A notable study focused on the cybersecurity issues within the hotel industry in Metro Dagupan, a major commercial center in Pangasinan (Bautista & Cerezo, 2021). The research indicated that while hotels were employing a range of cybersecurity tools such as firewalls, encryption, and physical security, and a majority had a dedicated cybersecurity team, the awareness and implementation of robust data protection practices were still evolving. The study underscored the critical role of cybersecurity in building and maintaining guest trust, with an overwhelming majority of both employees and guests agreeing that strong cybersecurity is a vital criterion in hotel selection (Bautista & Cerezo, 2021). This highlights a market-driven incentive for improving cybersecurity, but also implicitly points to the potential for significant reputational and financial damage in the event of a breach. The reliance on basic security measures may not be sufficient to counter more sophisticated and targeted attacks.

The findings from the Dagupan hotel industry can be extrapolated to other SME sectors in Pangasinan. These businesses, while increasingly reliant on digital tools for operations and marketing, often lack the financial resources and specialized expertise to implement comprehensive cybersecurity measures. They are consequently attractive targets for cybercriminals who perceive them as easier to breach than larger, more fortified corporations. The prevalence of online scams and business email compromise at the national level suggests that SMEs in Pangasinan are likely facing similar threats (The Asia Foundation, 2022).

Theme 3: The Role and Challenges of Academic Institutions

Higher education institutions in Pangasinan, such as Pangasinan State University, are central to the province's digital ecosystem. They are not only significant repositories of sensitive data (student records, research data, financial information) but are also responsible for cultivating the next generation of digitally literate citizens and cybersecurity professionals. The literature reveals that these institutions are both critical assets and potential points of vulnerability.

Research on the ICT infrastructure at PSU highlighted challenges such as unstable and poor internet connectivity and power interruptions, which directly impact the delivery of online education (Ventayen, 2019). While these are infrastructural issues, they have significant cybersecurity ramifications. An unstable network can hinder the implementation of consistent security updates and monitoring, creating windows of opportunity for attackers. Furthermore, the rapid shift to online learning during the COVID-19 pandemic, as detailed in studies on PSU's experiences (Cabansag & Ventayen, 2021), likely expanded the attack surface of the university's network, with numerous students and faculty connecting from less secure home networks.

On a positive note, academic institutions in Pangasinan are actively engaged in research that contributes to understanding the local digital landscape. Studies on digital literacy (Carpio, 2020), the challenges of online learning (Casimiro & Orlanda-Ventayen, 2024), and local industry practices (Bautista & Cerezo, 2021) provide valuable data for evidence-based policymaking. These institutions are also in a prime position to lead cybersecurity awareness and education initiatives, not just for their students but for the wider community. However, to effectively do so, they must first ensure their own digital infrastructures are secure and resilient.

Theme 4: The Overarching Influence of the National Cybercrime Landscape

While Pangasinan-specific cybercrime statistics are not readily available in the reviewed scholarly literature, the province is undoubtedly affected by the broader national trends. Research on cybersecurity in the Philippines paints a concerning picture of a dramatic increase in cybercrime incidents (The Asia Foundation, 2022). Online scams, in particular, have seen an exponential rise, becoming the most prevalent form of cybercrime in the country. Other significant threats include identity theft, phishing, and various forms of computer-related fraud.

A study assessing cybercrime awareness in another Philippine city, which can be seen as a proxy for the general urban experience in the country, found that while there is a general awareness of common cyber threats, a deeper understanding of the legal frameworks like the Cybercrime Prevention Act of 2012 (Republic Act No. 10175) is lacking (Tsakalidis & Vergidis, 2023). This gap between awareness and legal literacy can lead to underreporting of cybercrimes and a sense of impunity among perpetrators. It is reasonable to assume that the residents of Pangasinan share this national trend of being frequent targets of online scams and other cyber threats, while also facing similar challenges in seeking legal redress.

The national data also highlights the targeting of government agencies and critical infrastructure (The Asia Foundation, 2022). This suggests that local government units in Pangasinan, as well as essential service providers in the province, are potential targets. The need for robust cybersecurity measures at the local government level is therefore not just a matter of protecting data but of ensuring the continuity of public services.

In essence, the cybersecurity landscape of Pangasinan is a microcosm of the national situation, shaped by the pervasive threats of online fraud and the systemic challenges of inadequate digital literacy and a still-maturing cybersecurity infrastructure. The specific local studies from Pangasinan provide granular evidence that supports these broader national trends, confirming that the digital frontier in the province is fraught with both opportunities and significant risks.

Conclusion and Recommendation

This literature review has synthesized the available scholarly research to construct a preliminary understanding of the cybersecurity landscape in Pangasinan. The analysis reveals that while the province is actively participating in the national digital transformation, its journey is accompanied by a growing and multifaceted set of cyber risks. The thematic analysis of the literature underscores that the cybersecurity posture of Pangasinan is intrinsically linked to the digital literacy of its populace (Carpio, 2020; Cabansag & Ventayen, 2021), the preparedness of its local industries, particularly SMEs (Bautista & Cerezo, 2021), and the resilience of its academic institutions (Ventayen, 2019).

The findings indicate that a significant challenge for Pangasinan is the foundational issue of digital literacy. Research points to a need for enhanced digital competency not only among the general public but critically, among local government officials who are at the vanguard of e-governance initiatives (Carpio, 2020). The cybersecurity readiness of key local industries, such as tourism and hospitality, is another area of concern. While there is an emerging awareness of the importance of cybersecurity, the implementation of comprehensive and sophisticated security measures appears to be in its early stages, leaving many businesses vulnerable (Bautista & Cerezo, 2021). Academic institutions in the province are identified as crucial players, both as potential targets of cyberattacks and as vital centers for cybersecurity education and research. Finally, the cybersecurity experience in Pangasinan does not occur in a vacuum; it is heavily influenced by the escalating national trends in cybercrime, especially the proliferation of online scams and phishing (The Asia Foundation, 2022; Tsakalidis & Vergidis, 2023).

Based on the synthesis of the reviewed literature, the following recommendations are proposed to enhance the cybersecurity posture of Pangasinan:

1. **Develop and Implement a Provincial Cybersecurity Awareness and Education Program:** The provincial government, in collaboration with the Department of Information and Communications Technology (DICT), should spearhead a comprehensive and sustained public awareness campaign. This program should be tailored to different demographics, including students, the elderly, and local business owners. A key focus should be on practical skills such as identifying phishing emails, creating strong passwords, and understanding online privacy settings.
2. **Establish a Localized Cybersecurity Support System for SMEs:** Recognizing the resource constraints of small and medium-sized enterprises, a public-private partnership could be established to provide affordable cybersecurity services. This could include subsidized security audits, basic cybersecurity toolkits, and training workshops for business owners and their employees. The provincial government could partner with local universities and IT professionals to deliver these services.
3. **Strengthen the Cybersecurity Capacity of Local Government Units (LGUs):** A mandatory and regular cybersecurity training program should be instituted for all government employees in Pangasinan, with specialized training for LGU officials, building on the needs identified by research such as Carpio (2020). This training should cover data protection regulations, secure handling of sensitive information, and incident response protocols. The province should also consider creating a dedicated cybersecurity task force to coordinate security efforts across its municipalities and cities.
4. **Foster Academia-Industry-Government Collaboration:** A tripartite collaboration between Pangasinan's universities, local businesses, and the provincial government is essential. Universities can provide the research and expertise needed to understand the local threat landscape, while industry partners can offer real-world insights and internship opportunities for students, addressing the issues raised by Bautista and Cerezo (2021). The government can facilitate this collaboration and use the resulting research to inform evidence-based cybersecurity policies for the province.
5. **Promote Localized Research on Cybersecurity:** Academic institutions in Pangasinan should be encouraged and funded to conduct more in-depth research on the specific cybersecurity challenges and vulnerabilities within the province. This could include studies on the cyber risks to the local agriculture and aquaculture sectors, the effectiveness of different cybersecurity education strategies, and the socio-economic impact of cybercrime on Pangasinan households.

By taking these proactive steps, Pangasinan can move towards a more secure and resilient digital future, ensuring that the benefits of digital transformation are realized while mitigating the inherent risks of the ever-evolving cyber threat landscape.

REFERENCES

Ahmed, F., & Bures, M. (2023). A systematic review on the application of machine learning in digital forensics. Forensic Science International: Digital Investigation, 45, 301512.

Bautista, J., & Cerezo, A. (2021). *Cyber Security Issues in the Hotel Industry of Metro Dagupan*. Lyceum Northwestern University.

Cabansag, M. A. P., & Ventayen, R. J. M. (2021). The ecosystem of online learning in the Philippine setting: A case of Pangasinan State University. *Dialnet*, (21), 1-17.

Carpio, J. T. (2020). Digital Literacy among Elected Barangay Officials as an Input to a Community Extension Program. *SAJST*, *2*(1), 1-12.

Casimiro, R. R., & Orlanda-Ventayen, C. C. (2024). Challenges of Online Language and Literature Learning to the BSE-English Students of Pangasinan State University-Bayambang. *ResearchGate*.

The Asia Foundation. (2022). *Cybersecurity in the Philippines: Global Context and Local Challenges*. The Asia Foundation.

Tsakalidis, G., & Vergidis, K. (2023). Assessing Cybercrime Awareness and Experiences Among Netizen: A Study on the Impact of R.A. 10175 in Pagadian City. *International Journal of Research and Innovation in Social Science*, *IX*(V), 2786-2802.

Ventayen, R. J. M. (2019). Information & Communications Technology (ICT) Infrastructure Assessment of Pangasinan State University, Open University Systems. *ResearchGate*.

PLEASE INCLUDE CONTACT INFORMATION:
NAME: WENNA LYN D. HONRADO
CONTACT NO: +63 9129040877
EMAIL ADDRESS:
WLHONRADO_ASINGAN@PSU.EDU.PH