International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 9, pp. 3577-3590
doi: 10.25147/ijcsr.2017.001.1.234
https://stepacademic.net

Short Paper

Beyond Power Outages: The Cybersecurity Threat to the Electric Cooperatives in the Philippines and the Need for Data Privacy Awareness

Jaime Leonardo Bayobo
SGS, AMA University, Philippines
jaimeleonardobayobo@gmail.com
(corresponding author)

Richard Naje Monreal
SGS, AMA University, Philippines
richard.monreal@ama.edu.ph

Maksuda Sultana
SGS, AMA University, Philippines
maksuda.sultana@ama.edu.ph

Jenny Lyn Abamo
SGS, AMA University, Philippines
jlvabamo@amaes.edu.ph

Date received: June 8, 2024
Date received in revised form: January 13, 2024; February 9, 2025
Date accepted: February 16, 2025

Recommended citation:

Bayobo, J. L., Monreal, R., Sultana, M., & Abamo, J. L. (2025). Beyond power outages: The cybersecurity threat to the electric cooperatives in the Philippines and the need for data privacy awareness. *International Journal of Computing Sciences Research*, 9, 3577-3590. https://doi.org/10.25147/ijcsr.2017.001.1.234

Abstract

Purpose – The study explores the challenges faced by the 121 Electric Cooperatives in the Philippines in ensuring data privacy under Republic Act No. 10173 or the Data Privacy Act of 2012. Issues such as power outages and limited awareness of the DPA hinder the effective personal data protection for Member-Consumer-Owners (MCOs) and employees, despite the presence of Data Protection Officers (DPOs), which raises concerns about compliance with the law.

Method – Document analysis is used to examine data privacy challenges among the 121 Electric Cooperatives in the Philippines, drawing data from the National Privacy Commission (NPC), National Electrification Administration (NEA), and cooperative websites.

Results – A 2017 NEA memorandum urged electric cooperatives to comply with the Data Privacy Act of 2012 (DPA) and its regulations. While BENECO has implemented some measures, it lacks a designated DPO, a key requirement. In contrast, BATELEC II shows no clear evidence of DPA compliance on its website.

Conclusion – The study highlights the challenges Electric Cooperatives face in complying with the Data Privacy Act of 2012. Despite NEA's directives, disparities exist, with some cooperatives like BENECO showing documented efforts while BATELEC II lacks transparency in its compliance.

Recommendations – The NPC should implement stricter enforcement mechanisms to ensure data privacy compliance by electric cooperatives. The NEA and NPC should collaborate on capacity-building programs to educate electric cooperatives on data privacy best practices and compliance with the Data Privacy Act of 2012 (DPA).

Research Implications – Non-compliance with data privacy standards among electric cooperatives risks the personal information exposure of MCOs and employees. Addressing disparities through stronger enforcement and education is essential to data breach protection and prevention.

Keywords – Electric Cooperatives, Data Privacy Act of 2012, National Privacy Commission, National Electrification Administration, Data Protection Officer

INTRODUCTION

The Philippines, an archipelago nation striving towards digitalization, faces a crucial balancing act: harnessing the power of technology while safeguarding the privacy and security of its citizens' data. This tightrope walk becomes particularly important within the electric power sector, the lifeblood of a modern economy. The National Electrification Administration (NEA), tasked with overseeing the operations of Electric Cooperatives (ECs), plays a pivotal role in bringing electricity – and with it, the potential for digital integration – to a significant portion of the population, especially in far-flung areas (NEA, 2024). However, this progress comes with inherent risks.

ECs, entrusted with a vast amount of customer data – names, addresses, consumption patterns, and potentially even financial information – become prime targets for cyberattacks. A successful breach could have devastating consequences, exposing

sensitive information, and jeopardizing consumer trust (National Rural Electric Cooperative Association, 2024). This concept paper delves into the intricate relationship between the NEA, ECs, and the National Privacy Commission (NPC) in their joint effort to fortify cybersecurity and data privacy within the Philippine electric power sector. It aims to dissect the existing regulatory framework, identify potential vulnerabilities, and explore avenues for collaboration between these entities. Ultimately, this paper proposes strategies, tailor-made for the Philippine context, to bolster cybersecurity measures and cultivate a culture of data privacy compliance within ECs. By doing so, it aspires to safeguard consumer information, foster trust in the digital transformation of the Philippine electric grid, and pave the way for a more secure and empowered Filipino consumer in the digital age.

The National Electrification Administration, or NEA, is a government agency in the Philippines dedicated to bringing light to the countryside. Established in 1969, the NEA has been a key driver in rural electrification, working to improve the lives of Filipinos by providing them with access to a reliable and affordable electricity source (NEA, 2024). Through collaboration with electric cooperatives, the NEA has played a vital role in the social and economic development of rural areas throughout the Philippines.

In the Philippines, electric cooperatives (ECs) are non-profit organizations that bring affordable and reliable electricity to unserved areas. Founded in the 1960s with USAID, they're overseen by the NEA and are key to rural development. However, many ECs struggle with adopting modern technologies due to financial constraints and a lack of technical expertise, which makes them more vulnerable to cyber threats (Francisco et al., 2022).

On the other hand, the National Privacy Commission (NPC) is an independent body created under Republic Act No. 10173 or the Data Privacy Act of 2012. It is mandated to administer and implement the provisions of the Act and to monitor and ensure compliance of the country with international standards set for data protection (NPC, 2023).

The NPC safeguards the fundamental human right of every individual to privacy, particularly information privacy while ensuring the free flow of information to promote innovation, growth, and national development (Law.asia, 2022). It is attached to the Philippines' Department of Information and Communications Technology (DICT) for purposes of policy coordination but remains independent in the performance of its functions. Because ECs are non-profit organizations, budgeting is a major concern, especially when creating new positions in their staffing plans (Aroba, 2024). Limited funds also hinder innovation in both electric service and customer service, particularly regarding personal data protection. Existing staffing plans and technology may not be sufficient to adapt to the modern world, where the personal data of member-consumer-owners is at risk from hackers and scammers (Jaipong et al., 2023).

Better electricity and customer service are the voices of the member-consumer-owners nowadays, making an idea to privatize the electric cooperatives. Some Senators

expressed their opinions that electric cooperatives cannot operate (Philippine Star, 2023a). Some question the ECs' limited resources, which makes it difficult for them to implement new technologies and innovations compared to the private sector (Philippine Star, 2023b).

This concept paper proposes steps on how electric cooperatives can comply with the National Privacy Commission (NPC) to prevent data breaches and improve their cybersecurity.

LITERATURE REVIEW

Electric companies and utilities, including electric cooperatives, not only in the Philippines, encounter various cybersecurity threats. These threats, such as ransomware, phishing attacks, and system vulnerabilities, pose significant risks not only to electric services but also to the personal data of consumers. A cybersecurity threat was faced by the Colorado Electric Cooperative, as reported by America's National Rural Electric Cooperative Association (NRECA). The Colorado EC was hit by ransomware, affecting its network and taking over systems such as phone, email, meter data, and customer information (National Rural Electric Cooperative Association, 2024).

Schneider Electric also faces ransomware attacks on its sustainability division. Management confirms that the attack affected its Resource Advisor product and other division-specific systems. The management identifies the hackers behind the ransomware as the Cactus Ransomware Gang (The Record, 2023). These attacks may result from some employees lacking awareness of cybersecurity. In a recent report on The Philippine Health Insurance Corporation (PhilHealth) cyberattack, the NPC is assessing whether negligence was involved and if there was a possible concealment. The NPC identifies that the affected documents contain the personal information of the insured individuals (Philippine Star, 2023).

The PhilHealth cyberattack demonstrates that even a government-backed corporation from a developing country can be vulnerable to cyberattacks, potentially due to a lack of awareness regarding cybersecurity and the Data Privacy Act of 2012.

Contextual Analysis

The Electric Cooperatives in the Philippines operate under the regulation of NEA, the Department of Energy (DOE), and the Energy Regulatory Commission (ERC). Their primary goal as of 2024 is total rural electrification by the year 2028 under the Bagong Pilipinas administration. Despite being non-profit organizations, electric cooperatives often face challenges in adopting modern technologies, such as cybersecurity practices, and in implementing policies by the Data Privacy Act due to financial constraints and regulatory policies.

Cybersecurity Threats

Many cybersecurity threats can severely harm an electric cooperative's ability to carry out its business and provide sensitive information (Taylor & Ezekiel, 2024). The most glaring threat is malware, a blanket term referring to malicious applications that might damage or steal data or even gain unauthorized access to a system (Omorog & Medina, 2018). When an employee unintentionally clicks on a bad link or downloads an infected attachment, malware will be inserted into the system, granting the attacker full access to the employee's workstation, and by proxy, to the entire organization (Dela Rosa, 2023). Given the interconnectedness of their digital infrastructure, electric cooperatives are vulnerable to single breaches that easily spill over to cause widespread operational disruptions.

A common threat is Denial of Service (DoS) as well as Distributed Denial of Service (DDoS). These attacks overwhelm systems and networks, making them completely unavailable to the organization's consumers (Juneam & Greenlaw, 2024). For electric cooperatives, this can be impactful at three levels: service delivery could be affected, but moreover regulatory issues such as the Data Privacy Act 2012, especially the right-to-access policy, are similarly implicated (Jaipong, Siripipattanakul, Sriboonruang, & Sitthipon, 2023). Under this policy, consumers have the right to access their data at any time. This can be impeded by a DDoS attack, which erodes consumer trust and exposes the organization to regulatory penalties (Limna, Kraiwanit, & Siripipattanakul, 2023). In this context, the attacks are very impactful because of the increased reliance on online systems and web applications in the energy sector.

The second threat is SQL injection attacks that take advantage of vulnerabilities in the systems that an organization connects to its SQL databases. Hackers exploit such vulnerabilities by injecting malicious SQL code, which gives them a way to manipulate or steal data (Taruc & De La Cruz, 2024). Organizations that do not invest enough in their IT teams or disregard established protocols like the Software Development Cycle are at particular risk (Guerra, 2023). Electric cooperatives are at greater risk when using outdated or poorly maintained systems, as SQL injections may even compromise consumer information in addition to operational data (Rabano & Monreal, 2024).

Insider threats and ransomware add another layer of complication to the cybersecurity landscape. Insider threats are from employees, contractors, or partners who misuse their legitimate access to the systems, either for personal benefits or in conjunction with hacking from outside parties. It can leak sensitive information or create backdoors into systems (Balilo, Dioneda, & Byun, 2020). It can even destroy processes directly. Ransomware is another type of malware, which encrypts an organization's data and demands payment for its release. These attacks, often attributed to sophisticated hacker groups in China and North Korea, can cripple operations and cause significant financial loss (Bernabe & Junio, 2024). Together, these threats underline the urgency for electric

cooperatives to introduce strong cybersecurity measures, invest in employee training, and implement strict access controls over systems and data.

Factors Contributing to Lack of Awareness

Lack of cybersecurity and data privacy awareness in the electric cooperatives is one of the causes of the threats they experience since, through many factors, most organizations become vulnerable to certain attacks (Aroba, 2024). Among these are inadequate training programs and seminars about data privacy and cybersecurity. Thus, employees within that organization may not understand even a few words of either, leaving them helpless for anything they encounter as a potential danger to their respective organizations (Dong & Chen, 2024). With less proper training, even something so basic as spotting phishing attempts or choosing highly secure passwords could easily be missed, hence higher risks of breach (Banas & Mababa, 2023).

The antiquated IT infrastructure of many power cooperatives is yet another critical reason. Using old technology and software puts companies at risk as these systems may not be equipped with the latest security measures against ransomware, malware, and other risks (Hugo & Ngo, 2024). Critical security features like strong firewalls, anti-virus software, and anti-malware tools may be absent or inadequate. Those cooperatives that fail to develop and, subsequently, renew IT infrastructure remain favorable targets for hackers to exploit these weaknesses and gain illegal access to their personal information and systems (Francisco, Rodelas, & Ubaldo, 2022).

Another area where most electric cooperatives face a challenge is in data privacy requirements. The National Privacy Commission (NPC) requires the Data Privacy Act of 2012 to be followed strictly. This includes proper registration, the appointment of Data Protection Officers, and putting data protection safeguards in place (Acuna et al., 2024). Noncompliance exposes the company to administrative fines and penalties besides eroding its cybersecurity defenses. Lack of preparedness might trigger operational and reputational harm in that the NPC will randomly, unbudgeted do compliance checks on such entities-registered or not, or still non-compliant firms.

These combined challenges underscore the urgent need for electric cooperatives to prioritize cybersecurity and data privacy awareness. Investing in comprehensive employee training programs, upgrading IT infrastructure, and ensuring strict compliance with regulatory requirements are essential steps. By addressing these factors, cooperatives can strengthen their defenses against cyber threats, protect sensitive data, and maintain the trust of their member-consumer-owners and employees.

METHODOLOGY

The methodology of this study is a document analysis approach focusing on how the 121 Electric Cooperatives in the Philippines face data privacy challenges. This qualitative method includes an organized and interpretive scrutiny of numerous documents to deduce the patterns, themes, and insights associated with data privacy practices. The researchers obtained their data from reliable and relevant sources. These were mostly the available, publicly accessible documents available on the websites of the National Privacy Commission (NPC), the National Electrification Administration (NEA), and selected Electric Cooperatives.

The researchers first identified and compiled documents containing information on data privacy practices. They would have to navigate the official websites for regulatory guidelines, compliance updates, policy manuals, and any public records related to data privacy measures. These documents would become their main sources for analyzing how well the cooperatives have followed the Data Privacy Act of 2012 and to which extent there are gaps and inconsistencies in the implementation process.

The analysis involved comprehensive reading and coding of such content in the documents that were meant to deduce relevant information. Among elements such as Data Privacy Manuals, the appointment of Data Protection Officers, and even documents of compliance checks or reports, the study discovered patterns that would lead to the conclusion of whether it is possible for the cooperatives to align themselves toward data privacy requirements and, based on the patterns identified, what might be blocking its way toward compliance. The triangulation of information from these sources allowed the document analysis to provide a comprehensive understanding of the data privacy landscape in the electric cooperative sector. This method allowed the study to highlight disparities between practices and expectations of cooperatives and regulatory bodies while shining a light on systemic problems that need to be changed to improve data privacy compliance throughout the industry.

RESULTS

The study results indicate significant incongruities in data privacy compliance among cooperatives in the Philippines. Certain cooperatives, like BENECO, have data protection measures in place, one of which is a Data Privacy Manual. However, it lacks other critical points, such as the installation of a DPO. Conversely, other cooperatives, such as Batangas II Electric Cooperative, Inc. (BATELEC II), show no apparent observance of the Data Privacy Act of 2012 (DPA), indicating weaknesses in the sector's compliance with regulatory requirements. A few factors contribute to the challenges towards full compliance. Low budgets in non-profit cooperatives limit their investment in cybersecurity infrastructure, employee training, and seminars, and mostly, budget planning will usually compromise data privacy initiatives. In addition, cultural barriers exist due to a low level of computer literacy among employees in rural areas, making the implementation and sustainability of cybersecurity and data privacy practices complicated.

There are also regulatory dynamics with the National Electrification Administration (NEA) and the National Privacy Commission (NPC), which becomes a barrier. The main regulator for electric cooperatives, NEA sometimes is at odds with NPC's mandate to install a DPO. These overlaps in their regulatory framework cause delay and prevent compliance with efforts and require closer coordination of both agencies towards a smooth streamlining of data privacy compliance. Overall, the results reveal the pressing need for electric cooperatives to manage financial challenges, cultural gaps, and regulation pressures by focusing on budget management, proper and constant employee training, and enhancement of coordination with NEA and NPC in terms of security issues to safeguard personnel's personal information and maintain their cyber security.

DISCUSSION

The discussion about data privacy and cybersecurity challenges in the Philippine electric cooperative sector emphasizes the importance of targeted strategies. The importance of training programs and seminars lies in equipping employees with the knowledge and skills required to identify and mitigate potential cybersecurity threats. Funds are, therefore, allocated annually for regular training to reduce vulnerabilities by keeping staff abreast of the latest trends in data privacy and cybersecurity. A trained workforce reduces the risks of breaches and strengthens the reputation of the organization, thereby bringing trust from member-consumer-owners and stakeholders.

In addition, system updates should be done to harden the cybersecurity posture. Obsolete hardware and software are one of the easiest ways cyber-attacks penetrate an organization. Thus, constant updates are necessary. Inspired by the U.S. federal agencies' IT modernization efforts, electric cooperatives can also upgrade their systems by using the latest tools and technologies. This way, the systems will be resilient to evolving cyber threats and comply with global best practices in securing IT infrastructures. Compliance with the National Privacy Commission regulations is another essential element. Electric cooperatives must comply with the five pillars of compliance: appointing a Data Protection Officer, conducting Privacy Impact Assessments, and preparing a Privacy Management Program. Such compliance not only satisfies legal obligations but also provides strong frameworks for personal data protection. Implementation of data privacy governance and data breach protocols further enhances cooperatives' capabilities to detect, respond, and recover from security incidents efficiently.

These strategies, which include training programs, system upgrades, and strict compliance, will help electric cooperatives deal with the multi-dimensional challenges they face in terms of cybersecurity and data privacy. Such initiatives would be effective only if management, employees, and regulatory bodies are all working together to make these sustainable and effective. By investing consistently in education, technology, and governance, the cooperatives can build a secure environment that protects both their operations and the sensitive data of their stakeholders.

CONCLUSIONS AND RECOMMENDATIONS

This study points out significant challenges to Electric Cooperatives in the Philippines in complying with data privacy regulations. With the directives issued by the National Electrification Administration to ensure compliance of these cooperatives with the Data Privacy Act of 2012 (DPA), there remains a marked gap between the compliant and the non-compliant ones. While cooperatives like the Benguet Electric Cooperative (BENECO) have made substantial efforts to establish documented data privacy measures, others, such as Batangas II Electric Cooperative, Inc. (BATELEC II), have shown a lack of transparency regarding their compliance efforts. This disparity underscores the inconsistent application of data privacy practices across the sector.

The variation in compliance between electric cooperatives is alarming because it indicates that some organizations are not taking their responsibilities to protect sensitive personal data seriously. Cooperatives that do not implement data privacy measures put not only their operations at risk but also expose their members, including employees and consumers, to potential privacy breaches. For instance, cooperatives that do not publicly disclose their compliance or fail to establish clear privacy practices may inadvertently create vulnerabilities that cybercriminals can exploit. Such gaps in compliance may undermine trust and present long-term risks to the cooperatives and their stakeholders.

One of the major factors that lead to such disparities is the lack of consistent education and capacity-building efforts within the sector. Many electric cooperatives, especially those in rural settings, lack the resources, know-how, and training programs that will help them understand and enforce the Data Privacy Act fully. Consequently, while many cooperatives fail to institute thorough data privacy measures, a few cooperatives like BENECO have been successful. This calls for more targeted educational efforts and continuous support for cooperatives that do not have the in-house capability to meet the legal requirements set by the DPA. A stronger enforcement framework is necessary to address these challenges and ensure that all electric cooperatives comply with data privacy regulations. The NPC must take a more proactive role in monitoring and ensuring compliance across the sector. This could include conducting periodic and surprise audits of the electric cooperatives to monitor compliance with the DPA. Also, penalties should be uniformly imposed to oblige the cooperatives to consider data privacy seriously and not allow further violations.

Capacity Building and Co-Operation: Along with stricter enforcement, NPC and NEA shall join forces for capacity-building initiatives focused on educating the cooperatives regarding the best practices in the handling of data privacy. Such workshops, seminars, and online training courses will enable the cooperative staff to gain the knowledge and skills to successfully implement data privacy measures. Through these initiatives, there can be a development of compliance and awareness culture in the electric cooperative sector

to fill the gap between compliant and non-compliant cooperatives to ensure the protection of the personal data of all stakeholders involved.

IMPLICATIONS

The lack of data privacy compliance among electric cooperatives presents a serious risk to the personal information of member-consumer-owners and employees. As these cooperatives handle sensitive data, including personal and financial details, the absence of robust privacy measures increases the vulnerability of this data to misuse or theft. The disparities in compliance levels between different cooperatives further exacerbate the issue, with some cooperatives implementing necessary privacy practices while others remain non-compliant. This inconsistency can lead to confusion about which cooperatives are adequately protecting their data and may result in data breaches that harm consumers and damage trust in the sector.

To address these concerns, stronger enforcement of data privacy regulations is essential to ensure uniform compliance across all cooperatives. In addition to enforcement, there is a clear need for ongoing education and capacity-building programs for electric cooperatives. By equipping cooperative staff with the knowledge and tools needed to safeguard personal data, the industry can ensure better protection for its members and employees. A combination of stricter enforcement and enhanced education will help create a more secure and compliant environment in the electric power sector, reducing the risk of data breaches and fostering trust in these organizations.

ACKNOWLEDGEMENT

The authors wish to express their gratitude to the National Privacy Commission (NPC) and the National Electrification Administration (NEA) for their publicly available resources, which provided essential insights for this study. Special thanks go to the official websites of various electric cooperatives, which served as key sources of data for analyzing the current landscape of data privacy compliance. Finally, the authors acknowledge the support of their respective institutions, AMA University, for providing the infrastructure necessary for this research.

FUNDING

This study was conducted without financial support from any external institution. The research was entirely self-funded, with all necessary resources, including time, tools, and materials, provided by the researchers themselves. This independent approach allowed the researchers to maintain full control over the study's direction, methodology, and analysis, free from any external influence or bias.

The lack of institutional funding did not affect the quality or integrity of the study, as the researchers were committed to conducting a thorough and unbiased investigation. While external funding can provide additional resources, the study was able to proceed effectively through personal dedication and resourcefulness. This independent nature of the research highlights the researchers' commitment to contributing valuable insights to the field, even without financial backing from a sponsoring organization.

DECLARATIONS

Conflict of Interest

The researcher declares no conflict of interest in this study.

Informed Consent

No informed consent was collected since the study did not involve human participants or animals.

Ethics Approval

This study did not require ethics approval as it relied solely on publicly available documents.

REFERENCES

Acuña, C. A. A., Sabili, M. A., & Friginal, F. F. S. (2024). MARA: A Mobile-based Academic Reminder Application. *International Journal of Computing Sciences Research*, *8*, 2734-2748.

Aroba, O. J. (2024). Professional leadership investigation in big data and computer-mediated communication in relation to the 11th Sustainable Development Goals (SDG) global blueprint. International Journal of Computing Sciences Research, 8, 2592-2611. https://dx.doi.org/10.25147/ijcsr.2017.001.1.177

Balilo Jr, B. B., Dioneda Sr, R. R., Byun, Y., Balilo Jr, B. B., Dioneda Sr, R. R., & Byun, Y. C. (2020). Modified Transposition Using TDEA Encryption for FishCoral-PRSA Management System. *International Journal of Computing Sciences Research*, *5*, 584-594.

Bañas, J. C., & Mababa, J. C. (2023). File Integrity Verifier Using Digital Signature Algorithm and SHA-256 with Memory-Mapping Technique. *International Journal of Computing Sciences Research*, *7*, 2348-2357.

Bernabe Jr, R. Q., & Junio, O. M. (2024). Development of a Centralized Controlling System with Real-time Monitoring: Internet of Things, CCTV, Public Address, and FDAS: 4-

Systems in One Dashboard System using Raspberry Pi. *International Journal of Computing Sciences Research*, *8*, 2951-2970.

Dela Rosa, A. (2023). Web-based Management Information System of Cases Filed with National Labor Relations Commission. *International Journal of Computing Sciences Research, 7*, 1498-1513.

Dong, J., & Chen, T. (2024). Foreign Trade Company Personnel Management System using SSM Framework. *International Journal of Computing Sciences Research*, *8*, 2505-2535.

Francisco, R., Rodelas, N., & Ubaldo, J. (2022). The Perception of Filipinos on the Advent of Cryptocurrency and Non-Fungible Token (NFT) Games. *International Journal of Computing Sciences Research, 6*, 1005-1018

Global Government Forum. (2023, May 15). *US federal agencies to upgrade cyber and data capabilities as part of a government-wide IT plan*. Retrieved from https://www.globalgovernmentforum.com/us-federal-agencies-to-upgrade-cyber-and-data-capabilities-as-part-of-government-wide-it-plan/

Guerra, E. (2023). *Email attacks: An ensemble algorithm utilizing machine learning for phishing detection towards potential attack prevention*. Retrieved from IJCSR: https://stepacademic.net/ijcsr/article/view/452

Hugo, A., & Ngo, G. (2024). Private Blockchain-based Procurement and Asset Management System with QR Code. *International Journal of Computing Sciences Research, 8*, 2971-2983.

Jaipong, P., Siripipattanakul, S., Sriboonruang, P., & Sitthipon, T. (2023). A Review of Metaverse and Cybersecurity in the Digital Era. *International Journal of Computing Sciences Research, 7*, 1125-1132.

Juneam, N., & Greenlaw, R. (2024). Spawning Four-Year, ABET-Accreditable Programs in Cybersecurity from Existing Computer Science Programs in Thailand. *International Journal of Computing Sciences Research, 8*, 2612-2634.

Law.asia. (2022, May 6). *Revisiting data privacy in the pandemic*. Retrieved from https://law.asia/revisiting-data-privacy-pandemic/

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research, 7*, 1133-1151.

National Rural Electric Cooperative Association. (2024, May 15). *Along those lines: Delta-Montrose Electric Association cyberattack.* Retrieved from https://www.electric.coop/along-those-lines-delta-montrose-electric-association-cyberattack

Omorog, C., & Medina, R. (2018). Internet security awareness of Filipinos. *International Journal of Computing Sciences Research, 1*(4), 14-26.

Philippine Star. (2023, July 29). Privatization of ECs pushed. Retrieved from https://www.philstar.com/business/2023/07/29/2284542/privatization-ecs-pushed

Philippine Star. (2023, October 4). *Privacy Commission probes possible negligence in PhilHealth cyberattack.* Retrieved from https://www.philstar.com/headlines/2023/10/04/2301156/privacy-commission-probes-possible-negligence-philhealth-cyberattack

Rabano, C., & Monreal, R. (2024). Enhancing customer satisfaction through sentiment analysis and affect recognition using computer vision with predictive analytics for Blu Water Beach Resort & Parks. *International Journal of Computing Sciences Research, 8*, 3326-3336.

Schneider Electric. (2023, July 11). Schneider Electric confirms ransomware attack on sustainability division. Retrieved from https://therecord.media/schneider-electric-ransomware-attack-sustainability-division

Simplilearn. (n.d.). *The importance of security awareness training*. Retrieved from https://www.simplilearn.com/importance-of-security-awareness-training-article

Taruc, L., & De La Cruz, A. (2024). Narrowband-IoT (NB-IoT) and IoT use cases in universities, campuses, and educational institutions: A research analysis. *International Journal of Computing Sciences Research, 8*, 3042-3057.

Taylor, O., & Ezekiel, P. (2024). Firewall defense and response policy towards resisting attacks on network logs. *International Journal of Computing Sciences Research, 8*, 2886-2904.

Author's Biography

Jaime Leonardo Bayobo is a Database Administrator at Batangas II Electric Cooperative, Inc. (BATELEC II). His expertise spans database management, software programming, debugging, and resolving program-related issues. He has successfully presented and implemented innovations that improved the overall operational processes of BATELEC II. Currently, he is leading the development of an integrated CRM, Billing, and Collection System for the cooperative. He is dedicated to leveraging technology to enhance organizational efficiency.

Richard Naje Monreal is a Computer Engineering Professor at the Technological Institute of the Philippines, specializing in Information Technology. He has contributed to research in sentiment analysis, particularly focusing on educational pathways for senior high school students. His work includes developing frameworks for cyber threat intelligence sharing among colleges in Camarines Norte. Monreal's research interests encompass data analytics and decision support systems, aiming to enhance educational and technological infrastructures. He is dedicated to advancing the field of Information Technology through both teaching and research.

Dr. Maksuda Sultana is an Assistant Professor in the Computer Science Department at AMA University and Computer Colleges. She holds a Master of Science in Computer Science and a Doctorate in Information Technology. Her research interests include artificial intelligence and augmented reality. Dr. Sultana has contributed to the field through publications such as "A Deep Learning Algorithm for Mental Health Support using Artificial Intelligence," where she served as a research adviser. She is also recognized for her role in empowering the next generation of AI experts. Additionally, Dr. Sultana is among the 31

AMAES teachers who earned the CompTIA CySA+ Certification, demonstrating her commitment to advancing cybersecurity education.

Dr. Jenny Lyn V. Abamo is a respected academic affiliated with the AMA Education System in the Philippines, holding a Doctorate in Information Technology (DIT). She is recognized for her expertise in intelligent systems, data mining, and the development of cloud-based quality assurance models for higher education institutions. Among her notable works are predictive models for faculty selection using machine learning and innovative approaches to institutional quality assurance. In addition to her research, Dr. Abamo actively mentors graduate students and contributes to advancing IT education through her role at AMA University. Her dedication to academic excellence and innovation reflects her commitment to enhancing the educational landscape in the Philippines.