Navigating Cybersecurity Challenges in The Era of Digital Transformation: Threats and Mitigation Strategies in The Philippines

Paolo Gio G. Espiritu[1], Joefil C. Jocson[2]

[1]*Student, Master of Engineering Management, Graduate School, Nueva Ecija University of Science and Technology (NEUST), Cabanatuan, Nueva Ecija, Philippines.*

[2]*Professor, Master of Engineering Management, Graduate School, Nueva Ecija University of Science and Technology (NEUST), Cabanatuan, Nueva Ecija, Philippines.*

Corresponding Author: paologioespiritu@gmail.com

Abstract— **In the context of the ongoing digital transformation in the Philippines, this research seeks to navigate the cybersecurity landscape of the country. Employing a qualitative analysis approach, this study leverages a variety of data sources, including websites, news articles, official government documents, and research publications spanning from 2018 to 2023. The primary focus is on exploring the legal frameworks, regulations, mitigation strategies, and governmental programs aimed at securing the digital realm and protecting the financial assets and personal data of Filipino citizens. Furthermore, this research places particular emphasis on the identification of cyber threats and attacks occurring in the Philippines despite the presence of laws and mitigation strategies. It also addresses the challenges that impede the Philippine government's journey towards becoming fully cyberspace resilient during the digital transformation era.**

Among the significant findings is the recognition of legislative frameworks such as the Access Devices Regulation Act of 1998, the E-Commerce Act of 2000, the Cybercrime Prevention Act of 2012, the Data Privacy Act of 2012, the DICT Act of 2015, and the SIM Registration Act. These frameworks are designed to safeguard personal data, financial assets, and electronic transaction security and enhance cyberspace resilience. Additionally, the research uncovers the implementation of various programs and strategies aimed at strengthening the cybersecurity landscape and as support to the enforcement of the identified legal frameworks, such as the National Cybersecurity Plan, Computer Emergency Response Team, Budapest Convention on Cybercrime, National Security Policy (2023-2028), Cybersecurity Awareness Program (Training and Seminars), USAID's Better Access and Connectivity (BEACON) Project, and the observance of Cybersecurity Awareness Month. These legislative frameworks and government programs align with the demands of digital transformation and the ever-evolving cybersecurity landscape.

The study also highlights various cyber threats, including malware, DDoS attacks, SQL Injection Attacks, Insider Threats, Phishing, Supply Chain Attacks, and IoT-Based Attacks that have led to incidents in the country. These incidents include the Medusa ransomware attack on the PhilHealth Insurance website, multiple DDoS attacks on Philippines news websites during national elections, and the increasing incidents of phishing through SMS and email. Moreover, this research also identifies the challenges that act as impediments to the cultivation of a proficient cybersecurity workforce. Ultimately, this research produced valuable information and insightful analysis that concludes the current cybersecurity landscape of the Philippines in the era of digital transformation.

Index Terms— **Cybersecurity, Philippine Government, Cyber Attacks, Cyber Threats, Cybersecurity Challenges, Digital Transformation.**

1. Introduction

The rapid proliferation of digital technologies has ushered in a transformative era that impacts individuals worldwide. Our contemporary world is inundated with digital technologies that streamline daily routines and professional endeavors, yielding numerous opportunities and benefiting various sectors, including the economy, healthcare, and government. These positive impacts have been especially pronounced during the COVID-19 pandemic and continue to shape our lives today.

In the Philippines, a nation actively embracing digital transformation by transitioning from manual to digital processes and relying on internet-based and cloud-based solutions, these benefits are tangible. However, this sweeping digital transformation has concurrently exposed its citizens to a spectrum of cyber threats and cybersecurity challenges, extending beyond mere financial and operational risks to encroach upon national security and individual privacy.

Manuscript revised November 08, 2023; accepted November 09, 2023. Date of publication November 11, 2023.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898; SJIF: 5.59

Illustrating this vulnerability, recent data collected since November 2020 underscores the Philippines' current standing in cybersecurity literacy skills. According to the National Privacy Test results conducted by the cybersecurity company NordVPN, the Philippines ranks only 27th, reflecting a need for improvement in various aspects of online security awareness (Philstar.com, 2023). Additionally, the Philippines ranked 2nd in the 2022 global ranking of countries that experienced the most cyberattacks in that year, based on the number of web-based cyber threats detected and blocked by Kaspersky products (bworldonline.com, 2023). These rankings underscore the pressing need for cybersecurity enhancement within the Philippines.

As Filipinos continue to embrace digitalization, this inevitable exposure to various cyber threats necessitates a robust cybersecurity landscape within the country. This research aims to shed light on the legal frameworks and the mitigation strategies employed to boost cybersecurity in the country while embracing full digitalization. Also, this research aims to identify various cyber threats, recorded cyber-attacks, the impact of these attacks, and the challenges that hinder the country from becoming a cyberspace-resilient country.

To achieve the goal of this research, the research seeks to comprehensively explore the intricate cybersecurity landscape in the Philippines by addressing the following key research questions:

- What legislative frameworks are in place to support the cybersecurity landscape in the country, especially in the context of digital transformation?
- What strategies and approaches has the Philippine Government adopted in support of the implemented laws and regulations to effectively mitigate these cyber threats?
- What cybersecurity threats have been officially identified and acknowledged by the Philippine Government?
- What documented instances of cyberattacks have been reported and cataloged by the Philippine Government?
- What are the primary challenges and barriers in building a skilled and capable cybersecurity workforce in the Philippines?
- What are the economic and national security implications of cyberattacks and data breaches in the Philippines, and how do they impact the country's overall stability?

The output of this research, as a result of addressing each associated research question, will bring significant implications and benefits to the following:

- Enhancing Personal and Financial Data Protection: This research provides valuable insights into the cybersecurity landscape in the Philippines. Raising awareness about potential threats to personal and financial data and highlighting existing legal and strategic safeguards empowers Filipino citizens to protect their sensitive information better.
- Strengthening National Security: Through an in-depth analysis of existing threats, this study equips the Philippines with the knowledge needed to fortify critical infrastructure and government systems. By identifying vulnerabilities, the nation can develop a more resilient and impenetrable cybersecurity framework, thus safeguarding national security.
- Promoting Public Awareness and Education: Recognizing the role of individual users in cybersecurity, this research contributes to public awareness campaigns and educational initiatives. It encourages safe online practices among Filipino citizens, ultimately bolstering the overall cybersecurity posture of the nation.
- Ensuring International Compliance: To remain globally relevant, the Philippines must align its cybersecurity practices with international standards and regulations. This study offers guidance on meeting these standards, fostering international cooperation, and facilitating a more effective response to cyber threats.
- Facilitating Capacity Building: Effective cybersecurity relies on a well-trained workforce. This research provides valuable information about strategies, including government programs and training initiatives, aimed at addressing the skills gap and ensuring that the Philippines possesses a capable and skilled cybersecurity workforce.
- Influencing Policies and Regulatory Frameworks: Policymakers require data-driven insights to formulate effective cybersecurity policies. This study offers evidence-based recommendations, guiding the development of policies that can better protect the nation against evolving cyber threats.

Overall, this research will hold significant implications, spanning personal and financial data protection, national security, public awareness and education, international compliance, capacity building, and policy development. Its potential to inform policies, strengthen security measures, and contribute to the resilience of the Philippines against ever-evolving cyber threats underscores its paramount significance in the realm of cybersecurity within the country.

2. Methodology

This research employs a systematic approach to analyze existing data and materials to gain a comprehensive understanding of the current state of cybersecurity in the

Philippines.

The data utilized for this study spans the years 2018 to 2023. The data collection was conducted using a structured approach. A search strategy was devised to systematically retrieve relevant information pertaining to the research questions. Ethical considerations were paramount in this process, ensuring compliance with data privacy regulations and consent requirements.

The data sources utilized for this study include:

- News Articles: News articles from reputable sources were examined to provide real-time insights into cybersecurity incidents, trends, and developments in the Philippines.
- Research Publications: Academic and industry research papers were reviewed to gain in-depth insights into various facets of cybersecurity, including threats and implications of cyberattacks to the citizens and to the economy.
- Government Websites: Official government websites served as valuable sources of legislative frameworks, government strategies, and policy documents pertaining to information related to cybersecurity in the Philippines.
- Reports: Various reports, such as cybersecurity threat assessments and economic impact studies, were consulted to supplement the analysis with data-driven insights.
- Policy Documents: National and regional policy documents and strategies were scrutinized to gain an understanding of the government's initiatives in the field of cybersecurity.

The data collected from these sources was used to address the set of research questions that encompass legislative frameworks, government strategies, identified threats, documented cyberattacks, the cybersecurity workforce, and the economic and national security implications of cyber threats.

A qualitative content analysis approach was used in all collected data, which allowed for the systematic categorization and interpretation of data from the selected sources. This analysis method was chosen to identify trends, commonalities, and differences in the collected data. No specific software was used for data analysis, as manual interpretation was deemed appropriate for the qualitative nature of the study.

3. Results

A. Legal Frameworks to Support Cybersecurity Landscape in The Context of Digital Transformation:

1) E-Commerce Act of 2000

The "Electronic Commerce Act of 2000," formally designated as Republic Act No. 8792, was officially established on June 14, 2000. The complete text of this legislation is accessible through the Official Gazette of the Republic of the Philippines website. This law is designed to encourage the widespread adoption of electronic transactions within both government operations and among the general populace.

Electronic transactions, as defined in this act, encompass the utilization of electronic, optical, and similar mediums, modes, instrumentality, and technology to authenticate the authenticity and trustworthiness of electronic data messages or electronic documents. Notably, this legislation grants electronic documents the same legal validity as their traditional written counterparts, further advocating for the adoption of electronic signatures.

However, as the use of electronic transactions exposes users to various potential threats, Republic Act No. 8792 also defines and imposes penalties for illicit activities, including hacking or unauthorized access/interference in computer systems or servers and other activities outlined within the Act. In essence, this act endeavors to promote electronic transactions while concurrently upholding the principles of lawful access and data confidentiality throughout the transaction process.

2) Cybercrime Prevention Act of 2012

According to Republic Act No. 10175, commonly referred to as the "Cybercrime Prevention Act of 2012," which was promulgated on September 12, 2012, as documented on the Official Gazette of the Republic of the Philippines website, the primary objective of this legislation is to establish an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT). The intent is to facilitate unrestricted, accessible, and comprehensible access to the exchange and delivery of information while ensuring the protection and preservation of the integrity of computer systems, computer and communications networks, and databases, as well as the confidentiality, integrity, and accessibility of the information and data stored within them. To this end, the law deems it imperative to criminalize various forms of misconduct, misuse, abuse, and unlawful access, both domestically and internationally.

This legal framework encompasses a comprehensive range of offenses directed at the confidentiality, integrity, and availability of computer data and systems, including but not limited to unlawful access, unauthorized interception, data tampering, device misuse, cyber-squatting, and others. It prescribes corresponding penalties for individuals found guilty of these transgressions. In essence, the Cybercrime Prevention

Act of 2012 serves as a protective shield, safeguarding citizens from potential aggressors and individuals who may pose cyber threats with the intention of compromising their personal information and financial assets.

3) Data Privacy Act of 2012

Republic Act No. 10173, also recognized as the "Data Privacy Act of 2012," was officially ratified on August 15, 2012, with its publication detailed on the Official Gazette of the Republic of the Philippines website. This legislation, alternatively titled "An Act Protecting Individual Personal Information in Information and Communications Systems in The Government and The Private Sector, Creating for This Purpose a National Privacy Commission, And for Other Purposes," is primarily geared towards the protection of personal information stored within information and communications systems, encompassing both the public and private sectors.

The overarching objective of this law is to uphold the fundamental human right to privacy while concurrently facilitating the unencumbered flow of information, thereby fostering innovation and economic development. Chapter III of the act furnishes comprehensive directives for the processing of personal information, defining the parameters for its lawful collection, use, and dissemination. In tandem, Chapter V underscores the paramount significance of personal information security. This section advocates the adoption of technical measures to safeguard personal information against inadvertent or unlawful alterations, disclosures, or destruction. Additionally, it fortifies protection against cyber threats that may seek to compromise, delete, or pilfer the accumulated personal data.

4) Department of Information and Communications Technology (DICT) Act of 2015

The Department of Information and Communications Technology (DICT) is a national agency established by Republic Act No. 10844, also known as the "Department of Information and Communications Technology Act of 2015." The agency's primary responsibilities pertaining to cybersecurity revolve around safeguarding individuals' rights to privacy and the confidentiality of their personal information. Additionally, the DICT is tasked with ensuring the security of critical information and communication technology (ICT) infrastructures, including the information assets held by government entities, individuals, and businesses.

Under this legislation, the National Privacy Commission and the Cybercrime Investigation and Coordination Center serve as attached agencies to the DICT, assisting in the enforcement of cybersecurity measures and regulations and in the implementation of policies for data protection.

Among its key functions, the DICT is responsible for formulating the National Cybersecurity Plan, which outlines the country's strategic approach to cybersecurity. Furthermore, the DICT plays a pivotal role in the establishment and operation of the National Computer Emergency Response Team (CERT), an essential component of the nation's cyber defense infrastructure. Moreover, the department actively facilitates international cooperation in matters related to cybersecurity intelligence, strengthening the nation's cybersecurity posture on the global stage.

5) Access Devices Regulation Act of 1998

Republic Act No. 8484, recognized as the "Access Devices Regulation Act of 1998," received approval on February 11, 1998. Subsequently, Republic Act No. 11449, titled "An Act Providing for Additional Prohibitions to and Increasing Penalties for Violations of Republic Act No. 8484," introduced amendments to this legislation.

The primary objective of Republic Act No. 8484, as documented on the Official Gazette of the Republic of the Philippines website, is to establish a framework that safeguards the rights and defines the responsibilities of parties engaged in commercial transactions. This framework involves the regulation of the issuance and use of access devices, encompassing items such as credit cards, ATM cards, and similar instruments. The law's fundamental aim is to combat fraudulent activities and protect consumers by imposing penalties and prohibitions on unauthorized access device transactions. These offenses include card fraud, counterfeiting, and various forms of fraudulent practices.

The subsequent amendment, Republic Act No. 11449, introduced additional prohibitions and escalated penalties for violations outlined in the original legislation. The new prohibited acts included activities such as skimming, copying, or counterfeiting financial cards, producing or possessing software or hardware components for fraudulent purposes, unauthorized access to financial accounts, and hacking. These enhancements aimed to bolster the protection of consumer financial data and assets.

One notable amendment by Republic Act No. 11449 was the revision of penalties outlined in section 10 of Republic Act No. 8484, with the intention of imposing more stringent consequences on individuals engaged in prohibited activities.

Overall, the Access Devices Regulation Act of 1998, along with its amendments introduced by Republic Act No. 11449, holds significant relevance in the realm of cybersecurity. This legislation plays a pivotal role in imposing prohibitions and penalties to safeguard consumers and their financial information, contributing to the overall security of electronic financial transactions and assets.

6) *Subscriber Identity Module (SIM) Registration Act*

Republic Act No. 11934, also known as the "Subscriber Identity Module (SIM) Registration Act," received approval on October 10, 2022. As detailed on the Official Gazette of the Republic of the Philippines website, this legislation serves as a catalyst for responsible Subscriber Identity Module (SIM) use by mandating SIM registration through Public Telecommunications Entities (PTEs).

The primary objective of this law is to institute a system of SIM registration, thus facilitating the regulation of SIM utilization. It provides comprehensive guidelines for both the registration process and the subsequent responsible use of registered SIMs. Additionally, the act introduces penalties for violations that pertain to the Data Privacy Act and the Cybercrime Act in the context of SIM usage, including the implementation of prohibited activities.

This act was conceived primarily to address the escalating prevalence of cybercrime activities related to text messaging or SMS. It was formulated and ratified with the explicit goal of curbing the proliferation of phishing incidents via SMS. According to a report by the Philippine News Agency (Parrocha, 2023), prior to the implementation of this act, government bodies and National Telecommunications Commissions (NTCs) were inundated with approximately 1,500 daily complaints concerning text scam activities. However, following the enactment of this legislation, the same report indicates a significant reduction in text scam-related complaints, down to approximately 100 per day.

Republic Act No. 11934 plays a pivotal role in diminishing the number of individuals falling victim to SMS-related cybercrimes. It contributes to the enhancement of data security for users and the effective management of SIM activities, all geared toward thwarting prohibited actions that could compromise personal data and financial assets.

B. *Cybersecurity Strategies and Approaches of The Philippine Government:*

Aside from the laws and acts enacted, there are activities and strategies that the government explored to strengthen the Cybersecurity Landscape of the country. Here are some of the activities and strategies from the analyzed data:

1) *National Cybersecurity Plan*

The development of the National Cybersecurity Plan falls under the purview of the Department of Information and Communications Technology (DICT), in accordance with its mandate outlined in RA 10844. Currently, the government is governed by the National Cybersecurity Plan for 2017-2022. However, the DICT has already presented the National Cybersecurity Plan for 2023-2028 to the Cabinet, as reported by Inquirer.net (Mangosing, 2023). Secretary of the DICT, Sec. Uy, emphasized during the cabinet meeting that this new plan will identify critical infrastructures requiring security measures. It will also establish collaboration mechanisms among various civilian and military agencies to enhance the country's defense capabilities. Coordination efforts will be channeled through the National Cybersecurity Inter-Agency Committee (NCIAC).

The overarching goal of the National Cybersecurity Plan for 2023-2028 is to create a secure and dependable cyberspace for all Filipinos. According to opengov.com (Ocampo, 2023), this plan is structured around six key pillars:

- Enactment of the “Cybersecurity Act” to strengthen the policy framework;
- Secure and protect Critical Information Infrastructures (CII);
- Proactively defend the government and people in cyberspace;
- Operational and well-coordinated network of Computer Emergency Response Team (CERT) and SOC;
- Capacitate workforce in cybersecurity and enhancing international cooperation.

This plan underscores the importance of fostering a secure, trustworthy, and reliable online environment. It emphasizes the need for a Cybersecurity Act to address economic linkages and noncompliance with cybersecurity regulations. Additionally, it highlights the significance of collaboration across government agencies, facilitated through the National Cybersecurity Inter-Agency Committee (NCIAC), to coordinate cybersecurity initiatives.

As of now, the National Cybersecurity Plan for 2023-2028 is awaiting approval from the president.

2) *Computer Emergency Response Team (CERT-PH)*

In general, it is a team composed of information/cybersecurity experts that acts to impose strategies for the detection and protection against cybersecurity incidents. It functions to resolve cyber-related incidents and to provide guidelines for the proper response and handling of these incidents.

In the Philippines, the National Computer Emergency Response Team (CERT) operates as a division under the Cybersecurity Bureau of the Department of Information and Communications Technology (DICT). The primary mandate of this division is to handle the receipt, assessment, and response to reports and incidents related to computer security.

Additionally, the National CERT plays a crucial role in establishing and maintaining systematic information collection dissemination, as well as fostering coordination and collaboration among various stakeholders, particularly computer emergency response teams. The overarching goal is to effectively mitigate information security threats and manage cybersecurity risks within the nation's digital landscape (ncert.gov.ph)

3) Budapest Convention on Cybercrime

The Budapest Convention is a criminal justice treaty that offers immediate provisions to assist in the investigation and prosecution of cybercrime and cyber-related cases, as well as the collection of electronic evidence, regardless of the geographical location of the cases. These provisions apply specifically to the member states of the convention.

During the 17th Congress, the Senate Office released Resolution No. 89, which supported the country's accession to the Budapest Convention on Cybercrime. The Senate formally adopted this resolution on February 19, 2018. Later in the same year, President Rodrigo Duterte signed the accession, effectively incorporating the Philippines as a member of the Budapest Convention on Cybercrime, joining 56 other nations in this endeavor (Parrocha, 2018).

4) National Security Policy (2023-2028)

The National Security Policy (2023-2028) of the Philippines encompasses comprehensive plans and strategies aimed at ensuring the country's survival, progress, and resilience. Within the realm of cybersecurity, Chapter 3 of this policy articulates the overarching objective of national cyber resilience.

This chapter underscores the advantages of integrating technologies, including emerging ones, into the country's digital transformation endeavors. It highlights the importance of seizing the opportunities that digitalization offers. The Philippines is committed to institutionalizing this transformation into an E-Government, making investments in high-speed internet, digital technologies, ICT innovations, Artificial Intelligence, and other technological advancements.

Furthermore, the National Security Policy asserts that investing in cybersecurity is imperative to facilitate a smooth digital transformation while shielding the nation from cyberattacks and related threats. Strengthening the ICT infrastructure is deemed essential to bolster resilience in the face of digitalization risks. The policy also places emphasis on enhancing ICT training and education in critical areas, including cybercrime prevention, safeguarding critical infrastructure, raising cybersecurity awareness, fostering cyberattack readiness, and facilitating cyber incident response.

In summary, this chapter delineates the steps the Philippine government must take to achieve the goal of becoming a cyber-resilient nation, safeguarding its digital future in an increasingly interconnected world. ('National Security Plan 2023-2028,' 2023).

5) Cybersecurity Awareness Program (Training and Seminars)

The Department of Information and Communications Technology (DICT) offers training and seminars with the aim of enhancing the understanding and expertise of Filipinos in the field of Cybersecurity.

In a 2022 report by the Philippine News Agency, Secretary Ivan Uy of the Department of Information and Communications Technology (DICT) announced the agency's collaborative efforts with prominent technology companies such as CISCO, Oracle, Intel, and Microsoft to introduce Cybersecurity certification programs for the Filipino populace. Secretary Uy also revealed that the DICT had initiated partnerships with key educational institutions and authorities, including the Department of Education (DepEd), Commission on Higher Education (CHED), Technical Education and Skills Development Authority (TESDA), and state universities and colleges, to develop a broader range of courses within the field of Cybersecurity (Dela Cruz, 2022).

According to a report by CNN News in the same year, the DICT unveiled plans to offer concise training courses centered on Cybersecurity. The DICT had already initiated collaborations with private-sector partners to expand course offerings and certification programs.

Furthermore, the DICT had previously conducted several training sessions, as reported by the Philippine Information Agency (PIA) (Espinosa, 2023). Starting in 2020, the DICT Region 9 has been actively hosting free online webinars dedicated to Cybersecurity. This initiative aimed to address the growing cybersecurity threats by providing educational programs aimed at enhancing the country's cybersecurity preparedness. On March 14, 2023, the DICT Region 9 office received international recognition, the World Summit on Information Society Prizes 2023, from the International Telecommunications Union for its exemplary Cybersecurity education program.

In summary, the Department of Information and Communications Technology (DICT) has a comprehensive strategy in place to continue offering a wide array of training and seminars. These initiatives are intended to educate, train, and certify Filipinos, fostering greater awareness of Cybersecurity and cultivating cybersecurity expertise among the country's citizens.

C. The United States Agency for International Development (USAID), through its Better Access and Connectivity (BEACON) Project

The Philippines has formed a partnership with the United States through the United States Agency for International Development (USAID) with the overarching goal of fostering inclusive economic growth and promoting peace and stability within the country. USAID's approach centers on building the Philippines' self-reliance by bolstering its capacity to plan, finance, and execute its own development solutions (source: usaid.gov/Philippines).

As reported by the Philippine News Agency (Dela Cruz, 2022), USAID collaborates with various Philippine agencies, each with distinct purposes and objectives. In the realm of Cybersecurity, USAID joined forces with IBM to present an assessment report on the Philippines' current cyber workforce status on December 7, 2022. This report, titled "National Cybersecurity Talent Workforce Assessment Report of the Philippines," offers valuable insights into the nation's cyber workforce, prevailing challenges, and proposed solutions for addressing talent gaps and opportunities. One noteworthy revelation from the report is the shortage of cybersecurity professionals in the Philippines compared to other countries.

To address this pressing issue, USAID, through its Better Access and Connectivity (BEACON) Project, established a partnership with the Department of Information and Communications Technology. This partnership led to the launch of the Cybersecurity Proficiency Improvement Training (CPIT) program for government IT professionals on March 17, 2023. The CPIT Webinars are scheduled to occur on a monthly basis, covering a range of cybersecurity domains. These webinars are designed to augment the knowledge and skills of IT and cybersecurity professionals within the bureaucracy (source: Ronda, 2023).

In essence, this collaborative effort between the Philippines and USAID aims to bolster the country's cybersecurity workforce and capabilities, addressing critical skill gaps in the field of cybersecurity.

1) Cybersecurity Awareness Month

Proclamation No. 2054, documented on the Official Gazette of the Republic of the Philippines website, is an official proclamation originating from the Office of the President of the Philippines. This proclamation designates the month of September in the year 2010 and each subsequent year as "cybersecurity awareness month." Its central objective is to promote active engagement in the commemoration of this event by all government agencies, bureaus, offices, government-owned and/or controlled corporations (GOCCs) and their subsidiaries/units, as well as state universities and colleges (SUCs). The proclamation underscores the critical importance of cybersecurity information and seeks to heighten awareness regarding the significance of cybersecurity both within the government and across the wider community.

Subsequently, as reported by the Manila Bulletin in 2023, President Marcos issued Proclamation No. 353, shifting the country's observance of Cybersecurity Awareness Month from September to October. This proclamation, signed by Executive Secretary Lucas Bersamin on October 2, 2023, and released on October 4, 2023, aimed to align the Philippines with the international observance of 'Cybersecurity Awareness Month' in October. Under this new proclamation, the Department of Information and Communications Technology (DICT) was entrusted with leading the observance of Cybersecurity Awareness Month. The DICT was tasked with identifying programs, projects, and activities consistent with international best practices for the annual celebration. The overarching goal of Cybersecurity Awareness Month remains to strengthen efforts in addressing the strategic policy dimensions of cybersecurity, building a national cyber defense capability, and raising public awareness through intensified campaigns that highlight cybersecurity information (Geducos, 2023).

D. Cybersecurity Threats and Reported Attacks

Numerous cybersecurity threats have been recognized in the Philippines, reflecting the complex landscape of cybersecurity challenges faced by the country. This compilation presents a snapshot of some key cybersecurity threats, along with data detailing their occurrences, sourced from various web articles, government reports, and news sources:

1) Malware

Malware, a contraction of the term "malicious software," encompasses software crafted with the malicious intent of either exfiltrating sensitive data or causing harm to computer systems. Its capacity extends to compromising and impairing computers and their interconnected systems (Cisco.com, n.d).

Within the Philippines, Kaspersky, a prominent cybersecurity solutions provider, has disclosed that worms and viruses constitute the majority of malware instances that are locally detected and successfully thwarted on devices owned by Filipino customers and users. Astonishingly, Kaspersky's records reveal an astounding 25.06 million attempts at disseminating malware, positioning the Philippines as the second most targeted country globally in terms of cyberattacks (Ronda, R.A, 2023).

Another menacing strain of malware is Ransomware, which effectively takes hostage computer system access and demands a ransom in exchange for its release. The Unit 42 Ransomware and Extortion report illustrates that in 2022, there were eleven documented ransomware attacks, specifically targeting entities operating in manufacturing, professional services, legal services, and state and local government sectors. Noticeably, the Philippines ranked fourth among the countries most frequently targeted by ransomware groups in Southeast Asia during the same year (Crismundo, 2023).

Adding to this discourse, another report has revealed that the recently released State of Cybersecurity ASEAN report, produced in collaboration with cybersecurity solutions provider Palo Alto Networks (PANW), underscores the heightened concerns of Filipino organizations regarding the threat of malware attacks (Dado, N., 2023).

The most recent cyberattack, as reported on the Manila Bulletin news website, involved a ransomware attack known as Medusa and targeted the Philippine Health Insurance Corporation (PhilHealth). This incident occurred on September 22, 2023. According to the reports, this attack has the potential to impact around 65.05 million beneficiaries, based on records as of 2022, who were classified as direct contributors to PhilHealth (Samaniego, 2023). As a consequence of this attack, there was a data breach, and sensitive information was stolen. Additionally, reports from sources on the dark web revealed that documents taken from PhilHealth had been made available in online marketplaces, such as Telegram (Rosales et al., 2023), which subsequently resulted in a compromise of the health insurance members' data.

2) Distributed Denial of Service (DDoS) Attacks

A Distributed Denial of Service (DDoS) attack is a malevolent endeavor to disrupt the regular flow of traffic to a targeted server, service, or network by inundating the target or its surrounding infrastructure with an overwhelming volume of Internet traffic.

In 2021, the Philippines experienced the largest-ever volumetric DDoS attack on record.

On December 11 and 23, 2021, three prominent Philippine news websites—ABS-CBN, Rappler, and Vera Files—fell victim to DDoS Attacks. These attacks inundated their websites with an excessive volume of data traffic, rendering them inaccessible during those periods. While the perpetrators remained unidentified, experts suggested that the attacks were coordinated and possibly executed by a hired service (cpj.org, 2022).

Additionally, another DDoS attack was documented by the International Federation of Journalists (ifj.org, 2022). CNN Philippines encountered a cyberattack that rendered its site inaccessible to users while the network was hosting a presidential debate in preparation for the country's May 2022 election. It was speculated that the attacker's motive was to disrupt the election campaign that same year.

3) Phishing

Phishing, a prevalent form of cyberattack, involves malicious actors sending deceptive messages while impersonating trusted individuals or entities. These phishing messages manipulate unsuspecting users, inducing them to take actions such as downloading malicious files, clicking on harmful links, or divulging sensitive information like access credentials.

In the Philippines, phishing attacks have emerged as a prominent cybersecurity concern. In 2022, the country ranked fifth in Southeast Asia for the highest number of phishing attacks (Dagooc, 2023). These attacks primarily targeted users of delivery services, constituting 27.38% of all attempts blocked by Kaspersky Solutions. Scammers frequently employed emails and SMS messages, posing as reputable delivery companies and claiming issues with shipments. Each fraudulent email contained links to counterfeit websites, prompting users to provide personal or financial details. This tactic resulted in identity theft and data breaches, with stolen information often ending up for sale on various websites, particularly on the dark web.

Another report (Baclig, 2022) revealed that approximately 9.9% of Filipinos encountered phishing attempts. Phishing attacks were predominantly detected in three financial sectors: banks, e-commerce platforms, and payment systems.

Within the same report, it was disclosed that six teachers from various regions in the Philippines, including Metro Manila, Calabarzon (Cavite, Laguna, Batangas, Rizal, Quezon), Central Luzon, Negros, and Mindoro, reported losses ranging from at least P26,000 to P121,000 each due to unauthorized withdrawals from their payroll accounts at the Land Bank of the Philippines (LBP) in 2022. LBP denied any system hacking incidents and attributed the unauthorized access to phishing attempts.

4) SQL Injection Attack

SQL injection (SQLi) stands as a cyberattack method wherein malicious SQL code is surreptitiously inserted into an application. This nefarious practice permits attackers to gain unauthorized access to, view, or manipulate a targeted database. Notably, the Open Web Application Security Project (OWASP) recognized injection attacks, including SQL injections, as the third most significant web application security threat in 2021 (Crowdstrike.com, 2022).

In a noteworthy incident reported by the Manila Bulletin in 2021, the Bureau of Customs' website fell victim to an SQL injection attack. The attackers exploited a vulnerability they identified in the website's programming, allowing them unauthorized access. The culprits behind this attack were two hacking groups known as Pinoy Clownsec and Phantom Troup. Their objective was to expose the weaknesses within the website and deface the Bureau's online platform as a stark warning to the government about the precarious state of security in government websites (Samaniego, 2021).

5) Supply Chain Attack

A supply chain attack is a malicious strategy employed by threat actors to breach a target's system through the exploitation of vulnerabilities within third-party suppliers or vendors. These attacks come in two primary forms: software supply chain attacks, which introduce malevolent code into an application with the aim of infecting all users, and hardware supply chain attacks, which compromise physical components to achieve a similar objective (Crowdstrike.com, 2022).

An illustrative instance of a supply chain attack involves Philippine Airlines (PAL), where the attacker set their sights on Accleya, the airline's IT provider. In this breach, data associated with PAL's Mabuhay Miles frequent flyer program was compromised and fell into the hands of the malicious actor. The attacker leveraged third-party contractors affiliated with the airline to infiltrate the system. The data breach specifically affected customers who had enrolled in the Mabuhay Miles program between 2015 and 2017. Fortunately, the airline's internal systems remained unharmed in the aftermath of the attack. Nevertheless, as a precautionary measure, PAL urged its travelers to change their Mabuhay Miles passwords (cnnphilippines.com, 2022).

6) IoT-Based Attacks

An IoT attack encompasses any form of cyberattack directed at Internet of Things (IoT) devices or networks. When an IoT device is compromised, the attacker gains the capability to assume control over the device, exfiltrate data, or enlist it in a collective of infected devices, forming a botnet that can be used to launch Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks (Crowdstrike.com, 2022).

As the country increasingly integrates IoT technology into various aspects of daily life, numerous attacks have occurred, exploiting the inherent vulnerabilities in the IoT ecosystem.

In 2021, as reported by Business World Online (Balinbin, 2019), Kaspersky identified a total of 399 attacks targeting Internet of Things devices. These cybercriminals have been capitalizing on the perceived "weak security" of IoT products, viewing them as lucrative opportunities for exploitation.

Furthermore, a report from the Manila Times reveals that during the first two months of 2023, there was a disturbing trend where, nearly every week, approximately 54 percent of organizations experienced targeted attack attempts on their IoT devices. On average, each organization faced nearly 60 such attacks per week, marking a 41 percent increase compared to 2022 and more than a threefold surge compared to two years prior (manilatimes.net, 2023).

7) Insider Threats

Insider threats refer to the peril posed by individuals within an organization, which can include current or former employees. These internal actors present a significant risk to the organization due to their direct access to the company's network, sensitive data, and intellectual property (IP), and their familiarity with critical business processes, company policies, and other valuable information that can facilitate malicious activities (Crowdstrike.com, 2022).

Notably, the Philippines experienced an elevated exposure to insider threats during the pandemic. The surge in remote work arrangements, prompted by the need to avoid traffic congestion and reduce the risk of COVID-19 transmission, inadvertently increased the vulnerability of companies to insider threat attacks.

According to a report from PhilStar (Manantan, 2020), remote access to a company's confidential and proprietary data from employees' homes amplified the likelihood of "insider threats." These threats were categorized into three primary types:

- Careless or negligent employees or contractors constitute the largest portion of insider threats at 63%.
- Criminal or malicious insiders represent the second most prevalent type at 23%.
- Credential thieves occupy the smallest share at 13%

While no direct cyber-attacks were reported as a result of insider threats, the potential for data breaches and other security incidents loomed large due to the changing work landscape brought about by the pandemic.

E. Primary Challenges and Barriers to Building a Skilled and Capable Cybersecurity Workforce in The Philippines

1) Few Certified Cybersecurity Experts in the Country

According to a report by opengovasia.com, the Philippines has a relatively small number of certified cybersecurity experts, specifically individuals holding Certified Information Systems Security Professional (CISSP) certifications. Approximately 200 individuals in the country possess these certifications (Sathika, 2022).

2) Retaining Top Talents

Retaining top talents in the field of Cybersecurity poses a significant challenge for companies. According to a survey conducted by Fortinet, 63% of companies reported a shortage of skills in Cybersecurity, leading to severe consequences in terms of Cybersecurity incidents and vulnerabilities.

One noteworthy trend observed by Fortinet is that young talents who receive training and free certifications often leave their current companies, primarily enticed by better compensation packages or being recruited by other companies. (Piad, 2022).

3) Poor Digital Skills

In 2022, Assistant Secretary Jeffrey Ian Dy of the DICT shared the findings of a survey conducted on individuals aged 15 and above, focusing on digital literacy rates. The survey revealed that the digital literacy levels among the surveyed population were relatively low. Specifically:

- Basic Digital Skills (6%): Only 6% of the surveyed population possessed basic digital skills. These skills encompassed four activities, including copying or moving a file or folder, using copy and paste to duplicate or move information within a document or folder, sending emails with attachments, and transferring files between computers.
- Standard Digital Skills (2%): A mere 2% of the surveyed population had standard digital skills. These skills included using basic arithmetic formulas in a spreadsheet, connecting and installing new devices, creating presentations, and finding, downloading, installing, and configuring software.
- Advanced Digital Skills (1%): Only 1% of the surveyed population demonstrated advanced digital skills, particularly in areas related to programming and software engineering.

These findings underscored the need for comprehensive digital literacy initiatives and education programs to enhance the digital skills of the population, especially given the increasing importance of digital technology in today's world (mb.com.ph, 2022).

4) Low Cybersecurity and Data Privacy Awareness

The 2019 National ICT Household Survey revealed that cybersecurity and data privacy awareness among Filipinos was relatively low. Specifically, the survey found that only 44 percent of Filipinos had heard of cybersecurity and data privacy (Philippine Institute for Development Studies, 2021).

F. Economic And National Security Implications of Cyber Attacks and Data Breaches in The Philippines

Cyberattacks in the Philippines have raised significant concerns due to their potential economic losses and threats to national security.

Here are some forecasted and reported instances of such cyberattacks:

- 2016 Data Breach: In 2016, the Philippines suffered a significant data breach in which the personal information of 70 million voters was compromised. This breach, involving the Philippines Election Commission (COMELEC), raised concerns about its potential impact on the May 2020 elections. A 2019 study estimated that without improvements in cybersecurity, the country could face economic losses of up to $3.5 billion (Giray, 2022).
- Vulnerabilities to Foreign Cyberattacks: In a 2022 finance subcommittee hearing regarding the proposed 2023 budget of the Department of Information and Communications Technology (DICT), Senator Raffy Tulfo highlighted the vulnerability of the Philippines to cyberattacks from foreign countries, perceiving the country as a potential target. He expressed concerns about the possible impact of such attacks on critical infrastructure, including railway systems, communications, banking, and financial institutions. Additionally, there were fears of hacking during the election process, similar to what occurred during the 2016 US election (Felipe et al., 2022).
- Impact on Businesses: A 2022 Rappler report emphasized the significance of cybersecurity for economic security. The report revealed that 75% of businesses in the Philippines had experienced cyberattacks, resulting in an estimated daily loss of P6.16 billion due to such attacks (Gonzales, 2023).
- Losses in Critical Information Infrastructure (CII): Secure Connections ICT policy analyst and Better Internet PH lead advocate Mary Grace Mirandilla-Santos discussed the importance of securing critical information infrastructure (CII) in the Philippines. Top-listed companies operating CII faced potential daily revenue losses of PHP6.15 billion due to cyberattacks. The energy sector was identified as the most vulnerable, with daily potential losses of PHP2.8 billion, followed by banks (PHP1.5 billion), telecommunications (PHP1.06 billion), transportation (PHP631 million), water (PHP115 million), healthcare (PHP40 million), and other sectors (Crismundo, 2023).
- PhilHealth Cyberattack: On September 22, 2023, a cyberattack using ransomware targeted the website of the Philippine Health Insurance Corp. (PhilHealth).

This attack compromised private information and public health data. The cyberattack was attributed to the Medusa ransomware group, an international hacking group, which demanded USD300,000 to prevent the exposure of illegally obtained data (Bacelonia, 2023).

These reported incidents highlight the growing concerns surrounding cybersecurity in the Philippines and the need for enhanced measures to protect critical infrastructure, personal data, and national security.

4. Discussion

The Philippine government has established a robust legal framework to support its cybersecurity landscape within the context of digital transformation. Here are the key legislations found out by this research:

- E-Commerce Act of 2000 (Republic Act No. 8792): This act promotes electronic transactions, granting electronic documents the same legal validity as traditional ones. It also defines penalties for illicit activities, such as hacking, to ensure lawful access and data confidentiality.
- Cybercrime Prevention Act of 2012 (Republic Act No. 10175): Focused on facilitating the development and protection of information and communications technology, this act criminalizes various forms of cyber misconduct, aiming to safeguard computer systems, networks, and data.
- Data Privacy Act of 2012 (Republic Act No. 10173): This legislation protects personal information stored in information and communications systems, balancing privacy with the flow of information and advocating for technical measures to secure personal data.
- Department of Information and Communications Technology (DICT) Act of 2015 (Republic Act No. 10844): The DICT plays a central role in enforcing cybersecurity measures and regulations, formulating a National Cybersecurity Plan, and fostering international cooperation.
- Access Devices Regulation Act of 1998 (Republic Act No. 8484 and Republic Act No. 11449): This framework regulates the issuance and use of access devices, combats fraudulent activities, and protects consumers. The subsequent amendment increases penalties and prohibitions for unauthorized access device transactions.
- Subscriber Identity Module (SIM) Registration Act (Republic Act No. 11934): Mandating SIM registration through Public Telecommunications Entities (PTEs), this act addresses cybercrime related to text messaging, curbing the proliferation of text scams and enhancing data security for users.

These legal frameworks collectively aim to secure electronic transactions, protect personal data, combat and penalize cybercrime, and promote responsible access to digital resources. The Philippines has already made these legislations to strengthen its cybersecurity landscape, which supports its effort to embrace digital transformation.

Various initiatives were implemented and are currently in effect as mandated by the legislation and also in support of these laws. Here are the several programs and initiatives of the Philippine Government in relation to cybersecurity:

- National Cybersecurity Plan: The development of a comprehensive plan for 2023-2028 is awaiting approval, focusing on the "Cybersecurity Act," critical infrastructure protection, proactive defense, and international cooperation. It aims to create a secure digital environment for Filipinos.
- Computer Emergency Response Team (CERT-PH): CERT-PH plays a crucial role in incident response, information dissemination, and threat mitigation. It fosters collaboration among stakeholders for effective cybersecurity risk management.
- Budapest Convention on Cybercrime: Joining this international treaty enhances the Philippines' ability to investigate and prosecute cybercrimes, promoting global cooperation.
- National Security Policy (2023-2028): This policy integrates digital technologies into the country's development and highlights the importance of cybersecurity in digital transformation. Investment in ICT infrastructure and cybersecurity education is a priority.
- Cybersecurity Awareness Program: The Department of Information and Communications Technology (DICT) collaborates with private-sector partners and educational institutions to provide cybersecurity training and awareness programs.
- USAID Partnership: Collaboration with USAID aims to address skill gaps in the cybersecurity workforce with initiatives such as the Cybersecurity Proficiency Improvement Training (CPIT) program.
- Cybersecurity Awareness Month: The Philippines designates October as "Cybersecurity Awareness Month" to raise public awareness, emphasizing the importance of cybersecurity information.

These initiatives collectively reflect the government's commitment to protecting citizens and critical infrastructure from evolving cyber threats. The Philippines is actively striving to build a cyber-resilient nation in the digital age.

But even with these existing legal frameworks and mitigation strategies, the Philippine government still experiences various cybersecurity attacks:

- Malware: Malicious software, including worms, viruses, and ransomware, is a prevalent threat in the Philippines. The country ranks second globally in terms of cyberattacks, with millions of attempts to disseminate malware. Ransomware attacks targeting various sectors are a growing concern.
- DDoS Attacks: Distributed Denial of Service (DDoS) attacks have disrupted prominent news websites and even targeted critical events like presidential debates. These attacks, often coordinated, aim to disrupt services and create chaos.
- Phishing: Phishing attacks are widespread in the Philippines, particularly targeting users of delivery services. Impersonating reputable companies, attackers trick users into revealing personal and financial information, leading to identity theft and data breaches.
- SQL Injection Attacks: The Bureau of Customs' website fell victim to an SQL injection attack, emphasizing the importance of securing web applications against this type of cyberattack.
- Supply Chain Attacks: The compromise of data related to Philippine Airlines' frequent flyer program highlights the risks of supply chain attacks. Attackers leveraged third-party contractors to infiltrate the system.
- IoT-Based Attacks: As the Philippines integrates IoT technology into daily life, attacks on IoT devices have increased. Weak security in IoT products makes them attractive targets for cybercriminals.
- Insider Threats: The shift to remote work arrangements during the COVID-19 pandemic has increased the vulnerability to insider threats. These threats include careless or negligent employees, malicious insiders, and credential thieves.

These identified cyber threats and recorded cyber-attacks happened due to a lack of skilled and capable cybersecurity workforce and digital literate Filipinos, which was hindered by several challenges that were analyzed by this research:

- Few Certified Cybersecurity Experts: The Philippines has a limited number of certified cybersecurity experts, particularly those with CISSP certifications. With only around 200 individuals possessing these certifications, there is a shortage of skilled professionals in the field.
- Retaining Top Talents: Companies struggle to retain cybersecurity talents due to a shortage of skilled professionals. Many young talents leave their current positions in pursuit of better compensation packages or opportunities with other companies, contributing to skills shortages.
- Poor Digital Skills: A survey conducted by the DICT revealed that digital literacy rates among the population are relatively low. The majority lack basic and standard digital skills, hindering the development of a skilled cybersecurity workforce.
- Low Cybersecurity and Data Privacy Awareness: Cybersecurity and data privacy awareness among Filipinos remains low, with only 44 percent of the population having heard of these concepts. This lack of awareness poses challenges in building a cybersecurity-savvy workforce and society.

Addressing these challenges will require efforts in education, training, and awareness campaigns to develop a skilled and capable cybersecurity workforce in the Philippines. If addressed properly, these could prevent the economic and national security implications found by this study:

- Economic Losses: Cyberattacks result in significant financial losses for both businesses and the nation, potentially reaching billions of dollars.
- Foreign Cyberattack Vulnerability: The Philippines is susceptible to cyberattacks from foreign nations, which could target critical infrastructure, posing a threat to national security.
- Critical Information Infrastructure (CII): Protecting critical information infrastructure is vital, as cyberattacks on CII companies can lead to substantial daily revenue losses, particularly in sectors like energy, banking, and telecommunications.
- PhilHealth Cyberattack: Recent cyberattacks, like the one on PhilHealth, expose national security risks by compromising sensitive health data and engaging international hacking groups.

5. Conclusion

In summary, this research concludes that the Philippines has put in place a comprehensive legal framework to address a wide range of cybersecurity issues, encompassing electronic transactions, cybercrime prevention, data privacy, and the regulation of access devices and SIM cards. These laws collectively serve to safeguard personal data, financial assets, and the overall security of electronic transactions in alignment with the demands of digital transformation and the ever-evolving cybersecurity landscape. Furthermore, the research affirms that the country has implemented a variety of strategies and initiatives aimed at fortifying its cybersecurity environment, which complements the existing legal structures. These measures underscore the Philippine government's dedication to enhancing its cybersecurity readiness and safeguarding critical information infrastructure in the face of digital transformation and the evolving realm of cyber threats.

However, despite the presence of legal frameworks, acts, and proactive strategies, the research also highlights that the country has not yet attained true cyber resilience in this era of digital transformation. This is evident from recent notable cyberattacks that have resulted in the compromise of Filipino citizens' personal data, financial resources, and national security. The underlying causes of these security breaches can be attributed to several challenges that remain unaddressed or are still in the process of resolution. These include the need for increased public awareness regarding cybersecurity and how individuals can protect themselves from cyber threats, the imperative of retaining and upskilling a qualified cybersecurity workforce, and the underutilization of digital tools to prevent and mitigate various cyber threats.

In conclusion, there is a pressing need for the country to intensify its efforts in enforcing and implementing laws and regulations aimed at preventing and penalizing those involved in cybersecurity attacks. It is crucial to ensure the security of Filipinos' data and financial assets in the digital realm. Additionally, the government must expedite its initiatives to overcome the various challenges that hinder the development of a capable cybersecurity workforce and digitally literate citizens. Continuous government efforts are also essential in the form of additional programs and projects to bolster the cybersecurity landscape, produce more skilled and certified cybersecurity workforces, and promote internationally aligned cybersecurity standards and practices to achieve a fully cyberspace-resilient country.

References

[1]. Ronda, R.A. (2023, March 15). Philippines 2nd most attacked by web threats worldwide last year. Philippine Star.

[2]. "Philippines ranks second on global cyberattack list." (2023, March 16). Business World.

[3]. Republic Act No. 8792. (2000, 14 June). Official Gazette.

[4]. Republic Act No. 10175. (2012, 12 September). Official Gazette.

[5]. Republic Act No. 10173. (2012, 15 August). Official Gazette.

[6]. Republic Act No. 10844. (2016, 23 May). Official Gazette.

[7]. Republic Act No. 8484. (1998, February 11). Lawphil.

[8]. Republic Act No. 11449. (2019, 28 August). Official Gazette.

[9]. Republic Act No. 11934. (2022, 10 October). Official Gazette.

[10]. Parrocha, A. (2023, March 15). Marcos lauds nearly 100% decline in text scams due to SIM law. Philippine News Agency.

[11]. Mangosing, F. (2023, July 30). PH draws up 5-year cybersecurity plan. Philippine Daily Inquirer.

[12]. Ocampo, Y. (2023, May 29). The Philippines National Cybersecurity Plan Shaping a Secure Cyber Landscape. Opengov Asia.

[13]. National Computer Emergency Response Team. About Us. CERT-PH.

[14]. Parrocha, A. (2018, March 5). Palace lauds PH accession to cybercrime convention. Philippine News Agency.

[15]. National Security Policy (NSP) 2023-2028. (2023, August 10). National Security Policy Website.

[16]. Dela Cruz, R. (2022, December 20). DICT to launch courses on cybersecurity to build PH capacity. Philippine News Agency.

[17]. Espinosa, M.C. (2023, April 20). DICT Educates Netizens to Stay Cybersafe. Philippine Information Agency.

[18]. USAID. Philippines.

[19]. Dela Cruz, R. (2022, December 5). Usaid, Ibm to Present Report on Ph Cyber Talent Workforce. Philippine News Agency.

[20]. Ronda, R.A. (2023, March 7). Dict Gets Usaid Help on Cybersecurity. The Philippine Star.

[21]. Proclamation No. 2054. (2010, May 11). Official Gazette.

[22]. Geducos, A.C. (2023, October 5). Marcos Declares October as Cybersecurity Awareness Month. Manila Bulletin.

[23]. Cisco. What is malware?

[24]. Crismundo, K. (2023, March 22). Ransomware Attacks in Ph Jump By 57.4% In 2022. Philippine News Agency.

[25]. Lardizabal-Dado, N. (2023, September 24). Ph Tops Asean Cybersecurity Incidents List. The Manila Times.

[26]. Rosales, E.F & Felipe, C.S. (2023, October 6). Medusa Hackers Release Stolen PhilHealth Data. One News.

[27]. Samaniego, A. (2023, September 22). Philhealth Paralyzed by Medusa Ransomware Attack.

[28]. "Three Philippine Media Outlets Face Latest in a String of Cyberattacks." (2022, February 1). Committee to Protect Journalists.

[29]. "Philippines: CNN Philippines Hit by Cyberattack During Presidential Debate." (2022, March 4). International Federation of Journalists.

[30]. Dagooc, E. (2023, July 20). Philippines Ranks Fifth with Most Phishing Attacks In 2022. The Freeman.

[31]. Baclig, C.E. (2022, June 23). Ph Biggest Target of Phishing in Southeast Asia—Cybersecurity Report. Philippine Daily Inquirer.

[32]. "What is SQL Injection (SQLi)?" (2022, October 10). CrowdStrike.

[33]. Samaniego, A. (2021, March 13). Ph Bureau Of Customs Leaks Data Due to Poor Security. Manila Bulletin.

[34]. Baker, K. (2023, February 13). 10 Most Common Types of Cyber Attacks. CrowdStrike.

[35]. “Pal's Mabuhay Miles Suffers Data Breach”. (2022, September 11). CNN Philippines.

[36]. Balinbin, A. (2019, November 14). Malware Attacks on Iot, Android Devices in The Country Increase. Business World.

[37]. “Global Surge in Iot Cyberattacks Seen”. (2023, April 23). The Manila Times.

[38]. Manantan, M. (2020, May 4). As Employees Work from Home, Companies Are More at Risk Of ‘insider Threats’. Philippine Star.

[39]. Santhika, E. (2022, December 28). Building Cybersecurity Capability in the Philippines. Opengov Asia.

[40]. Piad, T.J. (2022, June 2). Ph Facing Shortage of Cybersecurity Talent. Philippine Daily Inquirer.

[41]. Dy, J.I (2022, August 25). Improving Digital Skills in the Philippines. Manila Bulletin.

[42]. "Infobits On Cybersecurity and Data Privacy Awareness in Ph". (2021, August 16). Philippine Institute for Development Studies.

[43]. Giray, J. (2022, January 1). Philippine Cybersecurity Market. International Trade Administration.

[44]. Felipe, C.S. & Romero, P. (2022, September 22). Tulfo Warns Vs Cyber Attacks, Danger to National Security. The Philippine Star.

[45]. Gonzales, G. (2023, June 9). US Embassy Says Cybersecurity Crucial in Economic Security. Rappler.

[46]. Barcelona, W. (2023, September 26). Senate Probe on PhilHealth Cyberattack Sought. Philippine News Agency.