NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE PHILIPPINES: CYBER THREATS

by

Lori M. Campbell

June 2023

Thesis Advisor: Wade L. Huntley
Second Reader: Tristan J. Mabry

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE THE PHILIPPINES: CYBER THREATS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Lori M. Campbell			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This research highlights the roles and functions of three government agencies responsible for cybersecurity policy and program coordination in the Philippines: the Computer Emergency Response Team Philippines Division under the Department of Information and Communications Technology, the Cybercrime Investigation and Coordinating Center, and the National Privacy Commission. These agencies' roles, functions, and mandates are described, including their responsibilities in incident response, data breach reporting, and enforcement of data privacy regulations. The research further analyzes five major recent data breaches: the Commission on Elections (2016), Jollibee Foods Corporation (2017), Wendy's (2018), Cebuana Lhuillier (2019), and the LuminousMoth Advanced Persistent Threat (2021) and evaluates the effectiveness of the government's response. While the Philippines has made progress in legislation, policies, and agencies that address cyber threats, challenges include timeliness in incident and data-breach reporting, coordination among government agencies and stakeholders, identifying offenders, improving cybersecurity awareness, and staying on top of the evolving nature of cyber threats. Overall, the research identifies areas for improvement such as implementing more robust security measures, regularly testing systems, investing in appropriate protection mechanisms, conducting drills and live training, and improving collaboration and information-sharing between organizations.

14. SUBJECT TERMS the Philippines, cyber, cybercrime, cyber threats, cyberattacks, cybercriminals, data breach, phishing, malware			**15. NUMBER OF PAGES** 95
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE PHILIPPINES: CYBER THREATS

Lori M. Campbell
Major, United States Marine Corps
BS, Fitchburg State University, 2010
MBA, Fitchburg State University, 2013
DBA, Northcentral University, 2020

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(EAST ASIA AND THE INDO-PACIFIC)

from the

NAVAL POSTGRADUATE SCHOOL
June 2023

Approved by: Wade L. Huntley
Advisor

Tristan J. Mabry
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research highlights the roles and functions of three government agencies responsible for cybersecurity policy and program coordination in the Philippines: the Computer Emergency Response Team Philippines Division under the Department of Information and Communications Technology, the Cybercrime Investigation and Coordinating Center, and the National Privacy Commission. These agencies' roles, functions, and mandates are described, including their responsibilities in incident response, data breach reporting, and enforcement of data privacy regulations. The research further analyzes five major recent data breaches: the Commission on Elections (2016), Jollibee Foods Corporation (2017), Wendy's (2018), Cebuana Lhuillier (2019), and the LuminousMoth Advanced Persistent Threat (2021) and evaluates the effectiveness of the government's response. While the Philippines has made progress in legislation, policies, and agencies that address cyber threats, challenges include timeliness in incident and data-breach reporting, coordination among government agencies and stakeholders, identifying offenders, improving cybersecurity awareness, and staying on top of the evolving nature of cyber threats. Overall, the research identifies areas for improvement such as implementing more robust security measures, regularly testing systems, investing in appropriate protection mechanisms, conducting drills and live training, and improving collaboration and information-sharing between organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
CERT	Computer Emergency Response Team
CERT-PH	Computer Emergency Response Team Philippines
CICC	Cybercrime Investigation and Coordinating Center
CID	Complaints and Investigation Division
COMELEC	Commission of Elections
DICT	Department of Information and Communications Technology
ICT	Information and Communication Technology
JFC	Jollibee Foods Corporation
NCERT	National Computer Emergency Response Team
NCSI	National Cybersecurity Index
NPC	National Privacy Commission
PRC	People's Republic of China

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to Dr. Huntley and Dr. Mabry for their invaluable contributions to this thesis. Their guidance, feedback, and patience have been instrumental. First and foremost, I would like to thank Dr. Huntley, my main advisor, for providing quick feedback in refining my ideas, methods, and results. I would like to acknowledge Dr. Mabry, who served as a reviewer for this thesis. His thoughtful feedback, constructive criticism, and valuable suggestions have helped us improve the quality of this thesis. Overall, Dr. Huntley and Dr. Mabry's unwavering support, dedication, and contributions have been instrumental, and I am honored to have had them as my thesis advisor and reviewer.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

The Philippine society has been increasingly dependent on cyberspace within the last decade. Thus, the Philippines has continuously dealt with cyberattacks without evidence of slowing down. The Philippines is left vulnerable to cyberattacks, expressing serious concerns about their effects on the Philippines government, businesses, and civilian population. Furthermore, these cyberattacks have threatened the Philippines' national security and interests. This thesis examines factors to answer the following research question: How effective has the Philippine government been in addressing cyber threats within its country?

B. SIGNIFICANCE OF THE RESEARCH QUESTION

The Philippines continues to face a growing number of cyber threats to individuals, companies, and corporate websites.[1] These include cybercrimes in the areas of identity and financial theft, the possession of confidential data, copyright violation, and website defacement. Cybercrime is when a computer system, the internet, public network, or private network is used to conduct illegal activities.[2] Cybercrimes include ineligible downloading, software piracy, hacking, and cyber coercion.[3] In addition, cybercrimes include theft, forgery, blackmail, fraud, and embezzlement conducted over the internet.[4]

---

[1] Amparo Fabe and Ella Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy," in *Routledge Companion to Global Cyber-Security Strategy*, ed. Scott N. Romaniuk and Mary Manjikian, (New York: Routledge, 2021), 315.

[2] Jia Li, "Cybercrime in the Philippines: A Case Study of National Security," *Turkish Journal of Computer and Mathematics Education* 12, no. 11 (May 2021): 4224, https://www.turcomat.org/index.php/turkbilmat/article/view/6550/5407.

[3] Ben Fermin Q. Abuda, Kareen Dionesia Rivera, and Roselle Valerio Noroña, "Predictive Validity of a Cybercrime Awareness Tool: The Case of Senior High School Students in a Philippine Secondary School," *International Journal in Information Technology in Governance, Education and Business* 2, no. 1 (January 2020): 18, https://ssrn.com/abstract=4007646.

[4] Li, "Cybercrime in the Philippines," 4227–8.

Cybercriminals typically use malware such as advanced persistent threat (APT), ransomware, trojan, and bots.[5]

Cybercrimes threaten the national protection and security of the Filipino people, privacy rights, private sectors, the government, and state order.[6] Cybercrimes compromise justice, safety, and security by producing false information or destroying evidence, filing false reports, modifying or deleting court records, threatening law enforcement judges and officers, and shutting down crime-reporting systems.[7] Cybercrimes undermine essential infrastructures, fiscal stability, the national economy, and both private and public sectors within the Philippines.[8] The expansion of technology, including social networks and mobile devices, created an ideal environment for cybercrimes and the dissemination of prohibited information on the internet.[9] Philippine businesses are concerned with the growing issues of cybercrime as cybersecurity and the protection of online servers lag.[10] Overall, the Philippines is dealing with an increasing number of cybercrimes that result in serious concerns.

Every year, an increasing number of Filipinos fall victim to malicious attacks and online criminal activities.[11] According to Iqbal Ramadhan, the Philippines was listed as the seventh most vulnerable state in cybersecurity in the world.[12] Similarly, the Philippines is considered at an elevated risk of cyberattacks and ranked eighth out of eighteen states

[5] Iqbal Ramadhan, "Building Cybersecurity Regulations in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)," *Journal of Social and Political Sciences* 3, no. 4 (December 2020): 988, https://doi.org/10.31014/aior.1991.03.04.230.

[6] Abuda, Rivera, and Noroña, "Predictive Validity of a Cybercrime Awareness Tool," 18; Li, "Cybercrime in the Philippines" 4224.

[7] Li, "Cybercrime in the Philippines" 4230.

[8] Li, 4224–30.

[9] Abuda, Rivera, and Noroña, "Predictive Validity of a Cybercrime Awareness Tool," 18.

[10] Philippines Crime and Security Risk Report Q1 2020, 23.

[11] Li, "Cybercrime in the Philippines," 4225.

[12] Ramadhan, "Building Cybersecurity Regulations in Southeast Asia," 988.

for financial and cybercrime risk within East and Southeast Asia.[13] FireEye—a cybersecurity company—identified the Philippines as the Association of Southeast Asian Nations (ASEAN) most exposed country to cyberattacks with services and consulting industries, government departments, high-tech firms, telecommunications, and entertainment companies as top targets.[14] Based on this information, the Philippines is behind, compared to other Asian countries, in its ability to deter these kinds of cyberattacks.

The Philippines also faces serious cyber threats beyond criminal attacks. In 2019, the Bureau of Customs reported unknown actors hacked its website, while websites of other government, military, educational institutions, and private organizations reported Pinoy LulzSec hacked their websites.[15] The hackers leaked files on military personnel and sensitive information.[16] These cases display Philippine government's reputational damage and operational costs regarding cybersecurity threats.

Perhaps most seriously for national security, the Philippines has been a target of cyberattacks from the People's Republic of China (PRC) due to their historical disputes of the South China Sea, a critical maritime location. Cyberconflicts between the two countries started in 2012 when the Philippines and the PRC were involved in a series of cyber conflicts following island disputes in the Spratly Islands and Scarborough Shoal.

In summary, the Philippines has a history of cyberattacks, making it vulnerable to cyber threats. The Philippine government is aware of the damage that cyberattacks cause but has not been able to deter such threats. This thesis analyzes the Philippines' cybersecurity posture and its effectiveness to respond to cyberattacks in order to identify strengths, weaknesses and areas for improvement. Further, this analysis determines how well public and private organizations have responded to the Philippine government's

[13] *Philippines Crime and Security Risk Report Q1 2020 in Fitch Solutions*, FSG 08789939 (London, UK: Fitch Solutions, 2019), 24, www.fitchsolutions.com.

[14] Philippines Crime and Security Risk Report Q1 2020, 25.

[15] Philippines Crime and Security Risk Report Q1 2020, 23–4.

[16] Philippines Crime and Security Risk Report Q1 2020, 24.

cybersecurity regulations and oversight. Last, this thesis further highlights the importance of cybersecurity based on the data collected.

C. LITERATURE REVIEW

1. Cyber Threats Against the Philippines

According to the literature, various actors have targeted the Philippines in cyberattacks. These attackers can be anywhere from those seeking to receive personal benefits and satisfaction to highly trained cybercriminals employed or contracted to accomplish specific cybercrimes.[17] However, there is a lack of scholarly information to pinpoint the main actors producing cyber threats against the Philippines. According to Mars Buan, a Philippine Automatic Data Processing Manager, China and Russia are the main actors that provide the most numbers in cyberattacks against the Philippines.[18] Although there was not any evidence identified in scholarly sources to support the claims of Russian cyberattacks, there were sources that identified cyberattacks coming from Chinese hackers.

Researchers have made similar efforts to pinpoint PRC cyberattacks against the Philippines. According to Mark Manantan, the Philippines, as a South China Sea rival of the PRC, has been a target of the PRC's cyberattacks, where several government entities and social media users have been infiltrated and influenced in favor of the PRC's interests.[19] The PRC's cyber operations against South China Sea rivals included espionage, data breach, infiltration, disinformation campaigns, and distributed denial-of-service as a way to advance the PRC's interests.[20] Moreover, researchers discovered the Philippines

[17] Li, "Cybercrime in the Philippines," 4227.

[18] Fabe and Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy," 316.

[19] Mark B. Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea," *Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs* 56, no. 3 (September 2020): 2, https://doi.org/10.1142/S1013251120400135.

[20] Manantan, "The People's Republic of China's Cyber Coercion," 3.

was a victim of anti-Philippines propaganda by the 1937 CN hacker group from China.[21] Thus far, the Philippines has been a victim of cyberattacks linked to the PRC, such as Luminous Moth, Chinese linked APT10, Operational Naval Gazing, malware called NanHaiShu, and several other cyberattacks after the 2016 ruling of the South China Sea Arbitration.

Chinese cyberattacks have interfered with Philippine politics, lawful disputes, military organizations, and critical infrastructure companies. According to Manantan, Chinese-linked hackers conducted cyber espionage activities and targeted critical energy, technology, transportation, telecommunication, and finance industries to acquire information related to territorial disputes.[22] Additionally, a Chinese APT group sent fake accounts and phishing emails to intelligence agency email accounts and targeted military and government officials in relation to the South China Sea dispute.[23] Findings revealed Chinese hackers were able to gain sensitive information, such as "general military documents, internal communications, equipment maintenance reports and specifications, event related materials, documentation of organizational programs and initiatives."[24] Consequently, the PRC was able to gain an upper hand ahead of diplomatic negotiations and conferences.

The Philippine government is aware of the PRC's cyberattacks but has not shown signs of retaliation specifically toward China. Since 2016, former Philippine President

---

[21] Gulizar Haciyakupoglu and Michael Raska, "China's Political Warfare in Taiwan Strategies, Methods and Global Implications," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, ed. Mikael Weissmann, Niklas Nilsson, Bj**ö**rn Palmerts, and Per Thunholm (London: I. B. Tauris, 2021), 194.; Inda M. Permata and Bima J. Nanda, "The Securitization of Cyber Issue in ASEAN," in a *2019 Proceeding of the 1st International Conference of ASEAN*, (Padang, West Sumatra, Indonesia. Warsaw: Sciendo, 2009), 91, https://doi.org.10.1515/9783110678666-012.

[22] Manantan, "The People's Republic of China's Cyber Coercion," 16.

[23] Manantan, 16.

[24] Manantan, 16.

Rodrigo Duterte has improved the Philippines' relationship with China[25] and perhaps did not want to take any actions to hinder the relationship. Instead, China and the Philippines have a bilateral agreement to enhance media cooperation through rebroadcasts, personnel exchanges, and joint productions of media content.[26] According to Bonny Lin et al., based on the information revealed in the 2020 social media disinformation campaigns, the authors suggest that Filipinos have been subject to pro-China disinformation through Instagram and Facebook.[27] As a result, the Philippine public may not be entirely aware of their vulnerability in relation to Chinese cyberattacks. In June 2022, President Bongbong Marcos assumed office, so the Philippine government may respond differently to Chinese cyberattacks.

Aside from cyber threats from Chinese actors, there is a lack of literature to pinpoint main actors conducting cyberattacks against the Philippines. Additional research may help identify both domestic and foreign cyber actors targeting the Philippines. Once these actors are identified then researchers may be able to identify their motives for conducting such cyberattacks. Researcher Jia Li mentions that cybercriminals lack fear in conducting illegal activity when there is no law enforcement or international legislation between countries to prosecute cybercrimes and the criminals involved.[28] If the Philippine government or other stakeholders publicly identify cybercriminals and prosecute them accordingly then conceivably others may beware to target the Philippines.

2. The Philippine Government's Response to Cyber Threats

Since 2012, the Philippine government has made several efforts to improve their cybersecurity efforts. For example, the Philippine government established the Cybercrime

---

[25] Bonny Lin, Cristina L. Garafola, Bruce McClintock, Jonah Blank, Jeffrey W. Hornung, Karen Schwindt, Jennifer D. P. Moroney, Paul Orner, Dennis Borrman, Sarah W. Denton, and Jason Chambers, Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific (Santa Monica, CA: RAND Corporation, 2022), 138, https://www.rand.org/pubs/research_reports/RRA594-1.html.

[26] Lin et al., *Competition in the Gray Zone*, 183.

[27] Lin et al., 183.

[28] Li, "Cybercrime in the Philippines: A Case Study of National Security," 4225.

Prevention Act of 2012 (RA 10175) to reprimand criminal offenses committed under information and communications technology.[29] In addition to the Cybercrime Prevention Act of 212, the Philippines enacted the Data Privacy Act of 2012. Robert Smith, Mark Perry, and Nucharee Smith stated,

> [The Data Privacy Act of 2012] is the policy of the state to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes…its inherent obligation to ensure the personal information in information and communication systems are secured and protected.[30]

Subsequently, the Philippine legislators passed Republic Act 10,844 – the Department of Information and Communications Technology (DICT) Act of 2015. Based on the act,

> The DICT shall be the primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national Information Communication Technology development agenda.[31]

The DICT includes the Cybercrime Investigation and Coordinating Center (CICC), which coordinates cybersecurity activities and facilitates cooperation, collaboration, support, and participation from stakeholders and international bodies in cybersecurity activities.[32] In 2016, the Supreme Court of the Philippines assigned special commercial courts as cybercrime courts to assist with prosecuting offenders and suppress data theft, hacking, and industrial espionage.[33] In 2018, the Supreme Court of the Philippines issued the Rule

---

[29] Aiken Serzo, "Philippine Regulations for Cross-border Digital Platforms: Impact and Reform Considerations," *Philippine Institute for Development Studies* 1, no. 1 (October 2021): 11, https://www.pids.gov.ph/publication/research-paper-series/philippine-regulations-for-cross-border-digital-platforms-impact-and-reform-considerations.

[30] Robert Smith, Mark Perry, and Nucharee Smith, "Three Shades of Data: Australia, Philippines, Thailand," *Singapore Journal of Legal Studies* 1, no. 1 (March 2021): 86, https://www.proquest.com/scholarly-journals/three-shades-data-australia-philippines-thailand/docview/2529334510/se-2?accountid=12702.

[31] Fabe and Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy," 315.

[32] Mamello Thinyane and Debora Christine*, Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies* (Macau: United Nations University, 2020), 56, http://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf.

[33] Philippines Crime and Security Risk Report Q1 2020, 25.

of Cybercrime Warrants (A.M. 17–11-03-SC), enabling law enforcement officers to investigate cybercrime offenses by disclosing computer data (e.g., traffic data, subscriber information, and other relevant data).[34] In addition, the Philippines established the Computer Emergency Response program that is responsible for providing government and private organizations preventative actions against cybersecurity threats.[35]

Over the last decade, the Philippine government has implemented several policies and programs to improve cybersecurity and hold persons accountable. Nevertheless, there is lack of empirical evidence to determine if these policies have been adequately enforced or benefitted the Philippines. Based on the Philippine National Cybersecurity Plan 2022 released in 2016, the Philippine government's primary goals were to protect critical information infrastructure, government networks, the supply chain of business, and individuals.[36] Still, there has not been any evidence to show that these goals have been met.

According to Serigne Diop et al., the Philippines requires resource owners to fix vulnerabilities and implement cybersecurity measures.[37] Under the Philippines' Cybercrime Act of 2012, it is an administrative and criminal offence to not correct security flaws and implement cybersecurity measures.[38] If this is the case, then it would be helpful to understand how cybersecurity measures are enforced and how successful organizations have been in following the Cybercrime Act of 2012. Teresa Camarines and John Camarines highlight local firms have not shown an increase in information technology budgets for

---

[34] Serzo, "Philippine Regulations for Cross-border Digital Platforms," 12.

[35] Thinyane and Christine, Cyber Resilience in Asia-Pacific, 56.

[36] Charmaine Misalucha-Willoughby and Francis Domingo, *Enhancing Australia-Philippine Cooperation: Diversifying Strategic Options* (Manila, Philippines: Stratbase *ADRi* Publications, 2019), 26.

[37] Serigne Diop, Jema Ndibwile, Doudou Fall, Shigeru Kashihara, and Youki Kadobayashi, "To Coerce or Not to Coerce? A Quantitative Investigation on Cybersecurity and Cybercrime Legislations Towards Large-scale Vulnerability Notifications," *IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, (October 2019): 286, https//doi.org/ 10.1109/ISSREW.2019.00085.

[38] Diop, Ndibwile, Fall, Kashihara, and Kadobayashi, "To Coerce or Not to Coerce? A Quantitative Investigation on Cybersecurity and Cybercrime Legislations Towards Large-scale Vulnerability Notifications," 283–4.

cybersecurity.[39] With cyberattacks in the rise, one would expect more spending on cybersecurity efforts.

According to researcher Francis Domingo, the Philippines' lack of cyber capabilities has prevented them from contributing to the security and stability of the regional cyberspace.[40] The Philippine state has been more focused on strengthening domestic law enforcement and military capabilities rather than responding to cyber threats.[41] Consequently, hackers and cybercriminals have launched cyberattacks within the Philippines due to its relaxed security measures and minimal number of secure internet servers.[42] The Philippines is an easy target for stealing money and data as online transactions and data often occur on unsecured servers rather than through encrypted technology.[43]

Therefore, more research is necessary to better depict the Philippine governments' cyber capabilities. Additionally, further research may examine the Philippine government's efforts in combatting and prosecuting domestic and foreign cybercriminals. Even though the Philippines is a part of the Asia-Pacific Economic Cooperation and ASEAN, there is relatively less research and analysis on whether and how the Philippine government is working with ASEAN partners and other states to address external cyber threats, making the Philippines' regional efforts less visible compared to their domestic endeavors.

Lastly, although China is conducting cyberattacks on the Philippines, other countries seem to be more worried about it than the Philippines itself. In scholarly sources, there is less attention than could be expected to the topic of the Philippines' response to

---

[39] Teresa Camarines and John Camarines, "Discussing data Security and Telehealth during the COVID-19 Pandemic," *Journal of Public Health*, (July 2021): 1, https//doi.org/10.1093/pubmed/fdab284.

[40] Francis Domingo, "Strategic Considerations for Philippine Cyber Security," *ADRInstitute for Strategic and International Studies* 8–9, no. 1 (January 2016): 6, https//doi.org/10.13140/RG.2.1.4636.7768.

[41] Domingo, "Strategic Considerations for Philippine Cyber Security," 9.

[42] Philippines Crime and Security Risk Report Q1 2020, 25.

[43] Philippines Crime and Security Risk Report Q1 2020, 25.

Chinese cyberattacks. The research for this thesis, including one of the five critical incidents investigated in this thesis, aims to fill this gap by elaborating more on Chinese cyberattacks that threaten the Philippines' national security.

3. Effectiveness of Government Responses

There has been considerable debate on whether Philippine government cybersecurity efforts have been effective. As noted above, the Philippines appears to be behind other Asian countries in protecting cyber security. But some researchers have found important points of progress as well.

According to Amparo Fabe and Ella Zarcilla-Genecela, risk awareness has increased within the Philippines as public and private sectors have increased their defensive measures.[44] Comparably, researchers Mamello Thinyane and Debora Christine observed that public awareness of cybersecurity within the Philippines has been raised through outreach projects, media campaigns, and national cybersecurity awareness month.[45] According to Thinyane and Christine, the Philippines is a more sophisticated country in incorporating cyber resilience in the national cybersecurity strategies by having evaluation mechanisms and measurement instruments to assess cybersecurity, cyber incident exercises, and a desired state of resilience.[46] Specifically, the Philippines has a well-established cybersecurity maturity model to assess cyber capacity and methods for improvement.[47]

According to the "Cisco 2018 Asia Pacific Security Capabilities Benchmark Study," which collected regional data from 2,000 respondents across 11 countries and global data from 3,600 respondents across 26 countries, 48% of defenders in the Philippines reported seeing fewer than 5,000 cyber breach alerts a day, which is better than

---

[44] Fabe and Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy," 315.

[45] Thinyane and Christine, Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies, 55.

[46] Mamello Thinyane and Debora Christine, *Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies* (Macau: United Nations University, 2020), 17, http://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf.

[47] Thinyane and Christine, Cyber Resilience in Asia-Pacific, 18.

the global standard of 44% and the regional benchmark of 31%.[48] Two-thirds of the alerts in the Philippines were false alarms, while 32% were investigated alerts.[49] This was lower than both the global (34%) and regional (44%) standards of investigated alerts.[50] In terms of responsiveness, the Philippines remediated 49% of the legitimate alerts, marking them slightly behind the global benchmark (50%) but the fourth highest within the region, with only India (52%), Japan (51%), and Australia (69%) outperforming the Philippines.[51] According to the findings, the Philippines was ahead of the globe and region in having lower numbers of cyber breach alerts and legitimate alerts but higher in false alarms. Furthermore, the Philippines displayed impressive results in remediating breach alerts.

Researchers Mamello Thinyane and Debora Christine reviewed the Asia-Pacific nation-states' National Cybersecurity Plan to determine each state's levels of commitment to cybersecurity (using the Global Cybersecurity Index), cyber maturity (using the Australian Strategic Policy Institute's Asia-Pacific Cyber Maturity Metric), and achievement in its social and economic dimensions (using the UNDP's Human Development Index).[52] Furthermore, that study analyzed additional sources to gain insights into the participation of these nation-states in international cybersecurity discussions, including their national cybersecurity authorities and CERTs.[53] The study assessed the level of commitment, cyber maturity, and achievement in the social and economic dimensions of the Philippines, which were ranked as medium (on a scale from low to high), 15th out of 25, and high (on a scale from low to very high) respectively.[54] Compared to neighboring countries, the Philippines has implemented stronger mandates to

---

[48] Cisco 2018 Asia Pacific Security Capabilities Benchmark Study: Regional Breach Readiness, (San Jose, CA: CISCO, 2018), 32, https://www.cisco.com/c/dam/global/en_au/products/pdfs/cisco_2018_asia_pacific_security_capabilities_benchmark_study.pdf.

[49] Cisco 2018 Asia Pacific Security Capabilities Benchmark Study, 32.

[50] Cisco 2018 Asia Pacific Security Capabilities Benchmark Study, 32.

[51] Cisco 2018 Asia Pacific Security Capabilities Benchmark Study, 32.

[52] Thinyane and Christine, "Cyber Resilience in Asia-Pacific," 10.

[53] Thinyane and Christine, 11.

[54] Thinyane and Christine, 11.

protect people's privacy, primarily through the Data Privacy Act.[55] Researcher Meelendra Singh compared key features of data privacy policies between Vietnam, Indonesia, and the Philippines. In this study, she discovered the Philippines and Vietnam provided data subjects the right to obtain a copy of data collected by the controller. In contrast, Indonesia did not provide data subjects the same rights.[56] In addition, the Philippines provided organizations with implementation guidelines on establishing a privacy program under the Data Privacy Act, while Vietnam and Indonesia did not provide such guidelines.[57] This study shows the Philippines has taken additional steps to protect data privacy compared to other countries in the Asia-Pacific region.

Christine Castillo says most developed states, including those with significant cyber capabilities, encounter cyber threats daily.[58] She argued that the Philippines' cybersecurity posture progressed within the last few years based on several accomplishments and challenges addressed.[59] For example, several pieces of legislation were developed, such as the Electronic Commerce Act of 2000, the Anti-Photo and Video Voyeurism Act of 2009, the Anti-Child Pornography Act of 2009, the Data Privacy Act of 2012, and the Cybercrime Prevention Act of 2012.[60] The Philippines implemented the DICT, CICC, NCERT, and the Philippines' National Cybersecurity Plan 2022. The Philippines was the first Southeast Asian country to join the Budapest Convention and has based its domestic legislation on cybercrime in the convention. As a catalyst for Southeast Asia, the Philippines actively contributed to the ASEAN ICT Master Plan 2020, Master

[55] Meelendra Singh, Understanding Data Privacy to Advance Customer Protection in Vietnam, Indonesia and the Philippines. (Bonn and Eschborn, Germany: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, 2020), 18, https://www.mefin.org/docs/data-privacy-report-vip.pdf.

[56] Singh, Understanding Data Privacy to Advance Customer Protection in Vietnam, Indonesia, and the Philippines, 40.

[57] Singh, Understanding Data Privacy to Advance Customer Protection in Vietnam, Indonesia, and the Philippines, 40.

[58] Christine Castillo, "Philippine Cybersecurity in Retrospect (2016-2021)," GOVPH, last accessed February 28, 2023, https://www.ndcp.edu.ph/philippine-cybersecurity-in-retrospect-2016-2021/#:~:text=In%20relation%2C%20a%202021%20study,capacity%20to%20manage%20cyber%20threats.

[59] Castillo, "Philippine Cybersecurity in Retrospect (2016-2021)."

[60] Castillo, "Philippine Cybersecurity in Retrospect (2016-2021)."

Plan on ASEAN Connectivity 2025, and the ASEAN Defence Minister's Meeting-Plus Experts Working Group on Cybersecurity.[61] The Philippine DICT has partnered with several private and public sectors, academic institutions, and industry practitioners.[62] Facebook, Microsoft, Voyager Innovations, Inc., State Grid Corporation of China, International Container Terminals Services, Inc., Union Bank, SyCip Gorres Velayo & Co., National Association of Data Protection Officers of the Philippines, De la Salle University, and the NPC are also partners.[63] The DICT and the Department of the National Defense launched the Cyber Bayanihan 2.0 project, involving information technology experts from various companies, aimed to secure critical cybersecurity infrastructure across the Philippines and combat current cybersecurity threats and cyberspace attacks.[64] These initiatives complemented the government's public-private partnership efforts to improve the country's cybersecurity defense capabilities.[65] Even though cybersecurity remains a vital concern, the Philippines has made several positive strides for improvement.

Based on the National Cybersecurity Index (NCSI)—a live global index (2023) that measures countries' cybersecurity capacities, such as preparedness to manage cyber incidents and prevent cyber threats, implemented by the central government—the Philippines ranked 45th out of 164 countries with an NCSI score of 65.64, outperforming the global average of 43.63.[66] Within East Asia, the Philippines ranked 5th out of 14 countries, exceeding the regional average of 45.92.[67] Table 1 displays the individual NCSI scores for all 164 countries.[68]

---

61 Castillo, "Philippine Cybersecurity in Retrospect (2016-2021)."

62 Fabe and Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy," 317.

63 Fabe and Zarcilla-Genecela, 318.

64 Fabe and Zarcilla-Genecela, 318.

65 Fabe and Zarcilla-Genecela, 318.

66 "National Cyber Security Index," E-Governance Academy Foundation Company, accessed March 11, 2023, https://ncsi.ega.ee/country/ph/.

67 "National Cyber Security Index."

68 "National Cyber Security Index."

Table 1. NCSI.[69]

Rank	Country	NCSI	Rank	Country	NCSI	Rank	Country	NCSI
1	Greece	96.1	**56**	Benin	58.44	**111**	Tanzania, United Republic of	24.68
2	Belgium	94.81	**57**	Qatar	58.44	**112**	Guatemala	24.68
3	Lithuania	93.51	**58**	Egypt	57.14	**113**	El Salvador	24.68
4	Estonia	93.51	**59**	Zambia	55.84	**114**	Tonga	23.38
5	Czech Republic	92.21	**60**	North Macedonia	55.84	**115**	Honduras	22.08
6	Germany	90.91	**61**	Iceland	55.84	**116**	Suriname	22.08
7	Romania	89.61	**62**	Uganda	54.55	**117**	Papua New Guinea	22.08
8	Portugal	89.61	**63**	Nigeria	54.55	**118**	Chad	20.78
9	Spain	88.31	**64**	Türkiye	54.55	**119**	Grenada	20.78
10	Poland	87.01	**65**	Ecuador	53.25	**120**	Bahamas	20.78
11	Finland	85.71	**66**	Tunisia	53.25	**121**	Liberia	19.48
12	Saudi Arabia	84.42	**67**	Colombia	53.25	**122**	Mali	19.48
13	France	84.42	**68**	Belarus	53.25	**123**	Senegal	19.48
14	Sweden	84.42	**69**	Brazil	51.95	**124**	Barbados	19.48
15	Denmark	84.42	**70**	China*	51.95	**125**	Lao PDR*	18.18
16	Croatia	83.12	**71**	New Zealand	51.95	**126**	Bhutan	18.18
17	Slovakia	83.12	**72**	Panama	50.65	**127**	Belize	18.18
18	Netherlands	83.12	**73**	Moldova (Republic of)	50.65	**128**	Mongolia*	18.18
19	Serbia	80.52	**74**	Malta	50.65	**129**	Somalia	18.18
20	Malaysia*	79.22	**75**	Costa Rica	49.35	**130**	Cuba	16.88
21	Italy	79.22	**76**	Kazakhstan	48.05	**131**	Zimbabwe	15.58
22	United Kingdom	77.92	**77**	Oman	45.45	**132**	Syrian Arab Republic	15.58
23	Switzerland	76.62	**78**	Sri Lanka	44.16	**133**	Cambodia*	15.58
24	Ukraine	75.32	**79**	Mauritius	44.16	**134**	Namibia	15.58
25	Latvia	75.32	**80**	Pakistan	42.86	**135**	Iran (Islamic Republic of)	14.29
26	Ireland	75.32	**81**	Kenya	41.56	**136**	Madagascar	12.99
27	Bulgaria	74.03	**82**	Jamaica	41.56	**137**	Saint Lucia	12.99
28	Dominican Republic	71.43	**83**	Brunei Darussalam*	41.56	**138**	Mauritania	11.69
29	Russian Federation	71.43	**84**	United Arab Emirates	40.26	**139**	Afghanistan	11.69
30	Singapore*	71.43	**85**	Indonesia*	38.96	**140**	Sudan	11.69
31	Morocco	70.13	**86**	Kyrgyzstan	37.66	**141**	Antigua and Barbuda	11.69
32	Canada	70.13	**87**	Mexico	37.66	**142**	Saint Kitts and Nevis	11.69
33	Austria	68.83	**88**	Vietnam*	36.36	**143**	Gambia	11.69
34	Korea (Republic of)*	68.83	**89**	Uzbekistan	36.36	**144**	Haiti	10.39
35	Bangladesh	67.53	**90**	South Africa	36.36	**145**	Samoa	10.39
36	Hungary	67.53	**91**	Armenia	35.06	**146**	Myanmar*	10.39
37	Israel	67.53	**92**	Montenegro	35.06	**147**	Tajikistan	10.39
38	Norway	67.53	**93**	Rwanda	33.77	**148**	Libya	10.39
39	Cyprus	66.23	**94**	Algeria	33.77	**149**	Guyana	10.39
40	Australia	66.23	**95**	Trinidad and Tobago	33.77	**150**	Seychelles	10.39
41	Luxembourg	66.23	**96**	Ethiopia	32.47	**151**	Angola	9.09
42	Thailand*	64.94	**97**	Cameroon	32.47	**152**	Mozambique	9.09
43	United States	64.94	**98**	Côte d'Ivoire	31.17	**153**	Yemen	7.79
44	Paraguay	63.64	**99**	Ghana	31.17	**154**	Burundi	7.79
45	Philippines*	63.64	**100**	Bolivia	31.17	**155**	Saint Vincent and the Grenadi	7.79
46	Argentina	63.64	**101**	Liechtenstein	31.17	**156**	Sierra Leone	7.79
47	Japan*	63.64	**102**	Nicaragua	29.87	**157**	Turkmenistan	7.79
48	Peru	62.34	**103**	Botswana	29.87	**158**	Congo (Democratic Republic	5.19
49	Albania	62.34	**104**	Nepal	28.57	**159**	Kiribati	5.19
50	Georgia	61.04	**105**	Venezuela	28.57	**160**	Iraq	5.19
51	India	59.74	**106**	Bosnia and Herzegovina	28.57	**161**	Dominica	3.9
52	Azerbaijan	59.74	**107**	Jordan	28.57	**162**	Solomon Islands	2.6
53	Chile	59.74	**108**	Malawi	27.27	**163**	Tuvalu	2.6
54	Uruguay	59.74	**109**	Vanuatu	25.97	**164**	South Sudan	1.3
55	Slovenia	59.74	**110**	Bahrain	25.97		**Total average**	**43.63**
							***East Asia average**	**45.92**

[69] Adapted from E-Governance Academy Foundation Company, "National Cyber Security Index."

Figure 1 displays the Philippines' NCSI fulfilment percentage. The index scored the Philippines high in its cybersecurity development, cyber threat analysis and information, protection of personal data, cyber incident response, and fight against cybercrime. The Philippines scored lowest in its contribution to global cybersecurity, protection of digital services, and protection of essential services. The Philippines was scored average to above average in education and professional development, e-identification and trust services, cyber crisis management, and military cyber operations.[70]

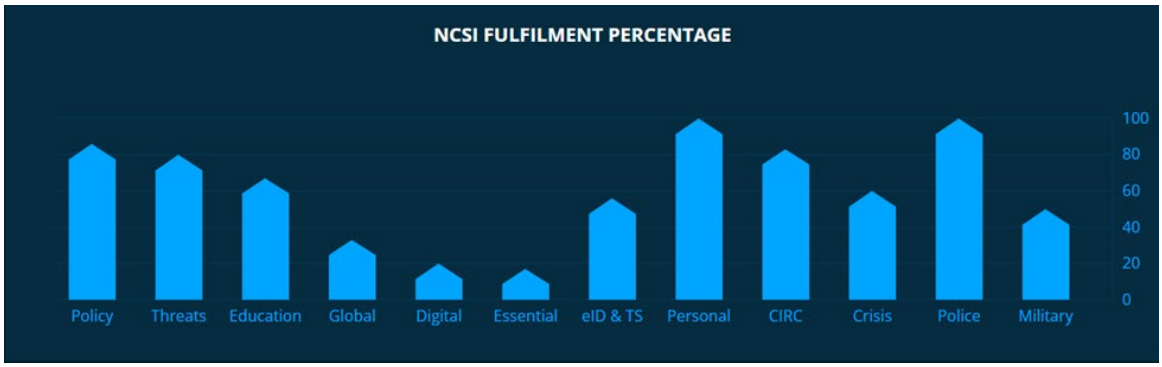

Figure 1. The Philippines' NCSI Fulfilment Percentage.[71]

The NCSI has shown that the Philippines has made significant progress in its cybersecurity capacities, and the government's efforts in developing cybersecurity measures have yielded positive results. Nonetheless, there are areas for improvement for the Philippine government to continue enhancing its cybersecurity capacities and be better equipped to address the ever-evolving cyber threats. Although some researchers believe the Philippines has made some great strides in cybersecurity, others have stated otherwise.

Economist Amparo Fabe and Chief Operating Officer Ella Zarcilla-Genecela highlighted several strategic, external, and internal challenges the Philippines face. First, the lack of talent and practical skills gap in cybersecurity remains a significant challenge for the Philippines. Second, the industry's fast-paced growth has left government officials

[70] E-Governance Academy Foundation Company, "National Cyber Security Index."

[71] Source: E-Governance Academy Foundation Company, "National Cyber Security Index."

ill-equipped to address its demands. Third, although risk awareness has increased within the Philippines as public and private sectors have increased their defensive measures, Filipinos still lack public awareness of cybersecurity risks. Fourth, the private sector has reduced its capacity to respond quickly to cyber-attacks and is unwilling to invest in appropriate protection mechanisms. Lastly, cybercriminals have access to more tools to commit more cybercrime, while the Philippines have difficulty identifying the source of cyber-attacks.[72]

Researcher Jia Li evaluated the impacts of cybercrime activities in public and private sectors in the Philippines, discovering cybercrime was an increasing problem for Filipino citizens, including public and private sectors. He emphasized key sectors, such as business process outsourcing, information technology, and banking and investment institutions, were particularly vulnerable to cybercrime, and stated,

> The government's inadequate approach to protecting companies will continue to affect investment…To make matters worse, the country's vulnerability towards such danger is also skyrocketing as the modernization of its critical infrastructure and economic systems calls for a stronger reliance on the computer network building on national and international scales.[73]

According to Li, the government's response to cybercrimes has been slow even though government websites and agencies have been hacked. Thus, public confidence in the government to deter cybercrimes has diminished.[74] The Philippines' cybersecurity policy governance has been uncoordinated and dispersed with actors operating in isolation from one another.[75] Cybercrime prevention has a small budget, ill-trained law enforcers, a lack of public awareness, and a lack of coordination and cooperation between private sectors

[72] Fabe and Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy," 322–323.

[73] Li, "Cybercrime In The Philippines," 4230.

[74] Li, 4230.

[75] Fabe and Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy," 322.

and the government.[76] Moreover, there is a lack of concern about escalating cybercrimes within the Philippines.[77]

However, Li failed to provide evidence of how the Philippine government has not responded to cybercrime activities. This suggests the author is assuming that the increased number of cybercrime activities and their effects results from an inadequate government approach without comparing it to other countries or the overall cybersecurity landscape.

Similarly, authors Inda Permata and Bima Nanda mention the development of information technology in the Philippines is not accompanied by an awareness of protecting it from cyberattacks.[78] The authors continue to state the Philippine government has not developed an adequate plan to deal with cyberattacks.[79] These statements are interesting since the National Privacy Commission (NPC)—a Philippine government department—had their fair share of complaints. The NPC noted that the Philippines is not at the level of developed nations when it comes to awareness in phishing, spam, and identity theft.[80]

Based on scholarly research, it is difficult to determine the effectiveness of government responses to cyber threats. Although the Philippine government has established cybersecurity strategy documents, policies, and programs to show their progress toward cybersecurity, their effectiveness is not measured or detailed in scholarly work. Therefore, this thesis evaluates the Philippine government's legislation and procedures to provide insight on their ability to respond to cyber threats. The thesis does so by evaluating a set of major historical cyberattack cases to determine how the Philippine government responded to the situation and the effectiveness of that response. In turn, the research conducted adds to the debate to whether the government responds effectively.

---

[76] Li, "Cybercrime in the Philippines: A Case Study of National Security," 4226.

[77] Li, 4226.

[78] Permata and Nanda, "The Securitization of Cyber Issue in ASEAN," 92.

[79] Permata and Nanda, 92.

[80] Smith, R., Perry, and Smith, N., "Three Shades of Data," 89.

D. POTENTIAL EXPLANATIONS AND HYPOTHESES

This thesis seeks to evaluate how effective the Philippine government has been in addressing cyber threats within its country. Perhaps the Philippine government has a solid cybersecurity strategy and plan, but executing such projects and enforcing their cybersecurity rules and regulations may lag. On the other hand, perhaps the Philippine government's cybersecurity strategy and plan could itself use improvement. In assessing the effectiveness of the Philippine government's cybersecurity efforts, the research for this thesis evaluates these two alternative hypotheses to better explain the sources of any inadequacies.

E. RESEARCH DESIGN

The research for this thesis first surveys the DICT's cybersecurity efforts, including those of their attached agencies, such as the NPC and CICC. Specifically, the research analyzes the reporting and response procedures of cyber threats. This analysis aims to determine if the Philippine government has deficiencies in its cybersecurity efforts and its ability to overcome cyber threats. Moreover, the research aims to determine if the Philippine government is providing proper oversight to ensure organizations follow mandated government cybersecurity policies. By providing a better understanding of the DICT, NPC, and CICC's cybersecurity efforts, including reporting and response procedures, this research serves as a foundation for analyzing the effectiveness of the Philippine government's actual responses to cyber threats.

Next, the research evaluates the Philippine government response to a set of significant cyberattacks in the Philippines. According to the Chief Information Officers of International Data Group Communications, the 2019 Cebuana Lhuillier marketing server breach, 2018 Wendy's data breach, 2017 Jollibee Foods Corporation (JFC) data breach, and 2016 Commission of Elections (COMELEC) government data breach were "the most serious data breach incidents in the ASEAN region during the past years."[81] In addition, the Center for Strategic and International Studies listed the 2021 LuminousMoth Advanced

[81] Cristina Lago, "The Biggest Data Breaches in Southeast Asia," CIO, last modified January 18, 2020, https://www.cio.com/article/222022/the-biggest-data-breaches-in-the-asean-region.html.

Persistent Threat (APT) as the most recent significant cyber incident that targeted the Philippines.[82] Therefore, this research study analyzes these five incidents of critical cyberattacks to develop evidence that enables a concrete evaluation of the effectiveness of Philippine government cyberattack responses.

For each incident, the research assembles information to answer the following sub-questions:

- Did the targeted organization report the cybercrime to the appropriate authorities?
- Did the Philippine government respond or provide any guidance to resolve the situation?
- If the Philippine government provided guidance, then was it followed?
- Was the problem resolved?
- Were the offenders identified? If so, who were they and what consequences did they face?

This research collects information from the Republic of the Philippines NPC and the DICT's Philippine National Computer Emergency Response Team (NCERT) to assist with answering the sub-questions for the five significant cyberattacks being analyzed. Altogether, the information retrieved and analyzed with the focus on these specific sub-questions generates the historical background, context, and basis for assessment of the Philippine government's cybersecurity efforts. Thus, the information retrieved helps create a better picture of whether the Philippine government's responses to cyber threats have been effective, and identify deficiencies of where those responses have fallen short.

[82] "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, 2022, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

F. THESIS OVERVIEW AND OUTLINE

This thesis consists of four chapters. Chapter I provides a brief overview of prior work related to cyberattacks and cyber vulnerabilities within the Philippines, including actions taken by the Philippine government to address cyber threats. Chapter II focuses on the Philippine government's cybersecurity procedures, depicting changes made within the last decade and whether they have been effective. Chapter III analyzes major cyberattacks within the Philippines while examining actions taken by the targeted organization and the Philippine government. Chapter IV provides the conclusion for this thesis, including the research summary, lessons learned, areas for improvement, research limitations, and areas for further research.

II. REPORTING AND RESPONSE PROCEDURES OF CYBER THREATS

A. INTRODUCTION

Computer and information security are critical to public and private organizations as they depend on information systems to pursue operational activities and objectives.[83] Nevertheless, information systems are vulnerable to threats, that result to adverse effects on an organization's operations, assets, and personnel,[84] making it essential for these threats to be detected and reported to the appropriate agencies. This chapter surveys the Department of Information and Communications Technology's (DICT) cybersecurity efforts, including those of their attached agencies, in particular the National Privacy Commission (NPC) and Cybercrime Investigation and Coordinating Center (CICC). Specifically, this chapter analyzes the reporting and response procedures of cyber threats. The information collected in this chapter shows whether the Philippine government has deficiencies in its cybersecurity procedures and practices.

B. DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

1. Overview

The DICT is "the primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national ICT development agenda."[85] The DICT's mission is to provide Filipinos access to critical ICT services and infrastructure, sustainable growth of Philippine ICT-enabled industries, and a one-digitized government by serving the following

[83] Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, (Quezon City, Philippines: Department of Information and Communications Technology, 2017), 11, https://www.ncert.gov.ph/cert-manual/dictcertmanual.pdf.

[84] Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, 11.

[85] Department of Information and Communications Technology, *Information Booklet*, (Quezon City, Philippines: Department of Information and Communications Technology, 2018), 3, https://dict.gov.ph/wp-content/uploads/2018/03/What-is-DICT.pdf.

functions: policy and planning, improved public access, resource-sharing and capacity building, consumer protection and industry development, cybersecurity policy and program coordination, and countryside development.[86]

Below lists the DICT's role under each function:

- Under policy and planning, the DICT formulates, recommends, and implements "national policies, plans, programs and guidelines" to "foster the development and use of ICT".[87]
- To improve public access, the DICT consults with local government groups, the private sector, academia, and civil society organizations to establish guidelines for the utilization and upkeep of ICT infrastructure.[88]
- For the DICT to implement "resource-sharing and capacity-building," the DICT synchronizes and coordinates "national ICT plans and initiatives," ensures the "development and protection of integrated government ICT infrastructures and designs," assists and provides technical expertise to government agencies, supports ICT research and development programs, prescribes personnel qualification standards, and disseminates critical information to reduce disaster risks via ICT.[89]
- The DICT oversees "consumer protection and industry development" by protecting "the rights and welfare of consumers" in ICT privacy, security, and confidentiality.[90]
- The DICT formulates cybersecurity policy and program coordination to minimize risks, cybercrime offenses, and cyberattacks against national

[86] Department of Information and Communications Technology, *Information Booklet*, 5–6.

[87] Department of Information and Communications Technology, 7.

[88] Department of Information and Communications Technology, 8.

[89] Department of Information and Communications Technology, 9–10.

[90] Department of Information and Communications Technology, 11.

security and critical infrastructures.[91] In addition, the DICT provides practical government countermeasures to address domestic and transnational incidents that threaten the Philippines' cyberspace and cybersecurity, as well as monitors cybercrime cases handled by law and prosecution agencies.[92]

- Last, the DICT provides countryside development by formulating policies to improve the provincial locations for the ICT industry and promote the development of ICT. The DICT also develops plans and programs to ensure universal access to ICT services. Further, the DICT assists, guides, and supports ICT-associated activities and initiatives for countryside economic development.[93]

Although the DICT provides several important functions for ICT, this chapter focuses on the DICT's cybersecurity policy and program coordination function as it offers immediate assistance to prevent real-time cyberattacks and coordinates effective measures to prevent cybercrime in reference to the Republic Act No. 10175 or Cybercrime Prevention Act of 2012 through a CERT. A CERT refers to

> an organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.[94]

2. Cybersecurity Policy and Program Coordination: Computer Emergency Response Team Philippines Division

DICT offers an incident response service through the Cybersecurity Bureau—Computer Emergency Response Team Philippines (CERT-PH) Division that delivers technical assistance for government agencies, critical information infrastructure sectors,

---

[91] Department of Information and Communications Technology, *Information Booklet*, 12.

[92] Department of Information and Communications Technology, 12.

[93] Department of Information and Communications Technology, 14.

[94] Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, 4–5.

external organizations, and other stakeholders in controlling a cyber-related incident in a way to minimize damage, recovery time, and costs.[95] The CERT-PH organizational chart is displayed in Figure 2.

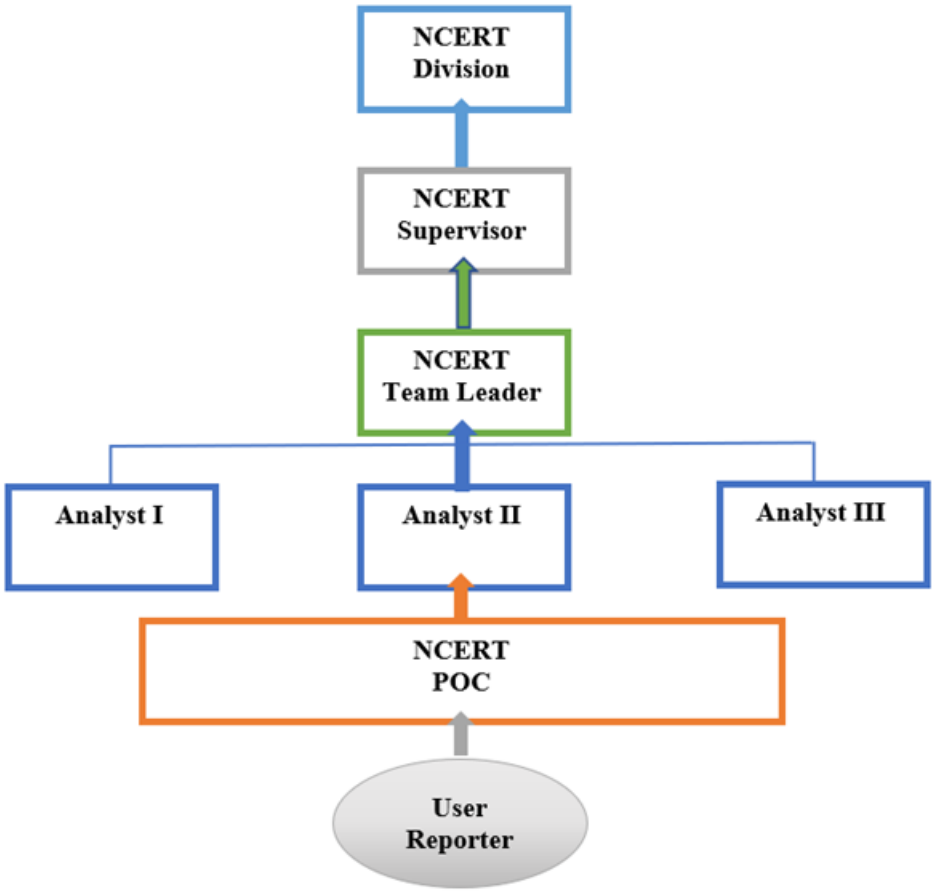

Figure 2. NCERT Organizational Structure.[96]

[95] Department of Information and Communications Technology, *Citizen's Charter*, 1st ed. (Quezon City, Philippines: Department of Information and Communications Technology, 2022), 86, https://dict.gov.ph/wp-content/uploads/2022/04/DICT-Citizen_s-Charter.pdf.

[96] Adapted from Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, Annex B.

The CERT-PH Division collects, reviews, and responds to computer security incident reports and activities.[97] The CERT-PH Division ensures systematic information gathering, dissemination, coordination, and collaboration between stakeholders and CERTs to alleviate cybersecurity risks and information security threats.[98] The primary functions of the CERT-PH division are to collect and gather data during the initial report of an incident, create initial information classification, "perform periodic reclassification," and "ensure regular reviews for value and updates to manage changes to risk."[99] Table 2 displays the CERT-PH Division's roles and responsibilities.

Table 2. NCERT Skills and Competency Framework.[100]

Role	Function	Duties and Responsibilities
POC	This level provides 24/7 frontline service for CSB in the implementation of the Computer Emergency Response which establishes the first POC with users or reporters of any detected incident or event.	1. Receive calls and act as the switchboard operator; 2. Screen and filter data for information classification; 3. Communicate relevant call to NCERT Team Leader; and 4. Provide administrative support to the operation of the team.
Analyst	Individuals assigned on this level perform analysis and evaluation of information to determine the relevance which will prompt immediate response and initiate series of actions to respond to the incident or event.	1. Initial collection and data gathering of information on detected and reported incident or event; 2. Creating initial information classification; 3. Opening and assigning incident report ticket number upon classifying information as relevant; 4. Closing of incident report ticket number when information is classified as false positive; 5. Communicating results to personnel or group of personnel with specific task to respond to the incident or event; 6. Perform appropriate responses with the immediate objective of deescalating level of vulnerability and adverse impact to the organization;

[97] Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, 9.

[98] Department of Information and Communications Technology, 9.

[99] Department of Information and Communications Technology, 9.

[100] Adapted from Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, 9–10.

Role	Function	Duties and Responsibilities
		7. Logging of responses and actions taken to update the database; and 8. File incident reports on assigned cases.
Team Leader	Individuals assigned on this level perform supervision and evaluate reported incidents before assigning caseloads to Analyst with appropriate set skills in performing analysis and evaluation of the data gathered and collected during the initial reporting stage.	1. Assign caseloads to NCERT Analyst; 2. Ensure regular review for value and updates to manage changes to risk; 3. Monitor close/open incident report ticket, resolved/unresolved incidents or events; 4. Ensure that appropriate responses are immediately implemented and communicated to personnel tasked to perform specific roles; 5. Ensure that frontline personnel and analysts log and update records immediately and accordingly; 6. Makes the decision to escalate or de-escalate incidents per assessment; 7. Evaluate the performance of Analysts and POCs; and 8. Prepare summary of daily reports.
Supervisor	Personnel assigned on this level supervise the NCERT team and external groups assigned to perform support services in responding to information security incidents or events.	1. Interface and report to the Director a summary of incident response activities and series of actions taken by NCERT; 2. Evaluate the performance of the NCERT Team Leader to assess efficiency of responses and the effectiveness of the established guidelines, procedures, and processes; 3. Regular review of collected and gathered data to evaluate information value; 4. Submit summary of resolved and unresolved cases to the management for input during review and improvement of the information security incident response plan; 5. Submit analysis results of incidents classified as false positive for input during review to determine the capability of frontline personnel in collecting and gathering substantial information; 6. Evaluate competency of personnel assigned to NCERT to recommend training programs

Role	Function	Duties and Responsibilities
		development for competency building of the NCERT Team; and 7. Prepare reportorial requirements for operational, administrative and budgetary purposes.

Cybersecurity incidents that compromise an information system's availability, confidentiality, or integrity are to be reported to the CERT-PH.[101] Incident reports that do not necessarily affect the information system, such as phishing attempts, passive scans, thwarted exploits, or attempted access, may be voluntarily submitted to the CERT-PH.[102] Stakeholders can submit a technical assistance request form to the CERT-PH to receive incident response support, cyber threats monitoring, and investigation.[103] Table 3 displays the step-by-step process to submit an incident report and technical assistance request form. Table 4 displays cyber threat levels and the required reporting timeframes for cybersecurity incidents based on their description. The DICT ensures external groups are aware of CERT services by providing them with adequate information, brochures, materials, and excerpts from the DICT CERT manual that describes the CERT's purpose and services offered.[104]

[101] Department of Information and Communications Technology National Computer Emergency Response Team, *CERT-PH Incident Reporting and Technical Assistance Request Guidelines*, Version 1.0. (Quezon City, Philippines: Department of Information and Communications Technology, 2020), 2, https://www.ncert.gov.ph/wp-content/uploads/2020/06/CERT-PH-Incident-Reporting-and-Technical-Assistance-Request-Guidelines.pdf.

[102] Department of Information and Communications Technology National Computer Emergency Response Team, *CERT-PH Incident Reporting and Technical Assistance Request Guidelines*, 2.

[103] Department of Information and Communications Technology National Computer Emergency Response Team, 2.

[104] Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, 3.

Table 3. Request for Incident Response Service.[105]

Step	Required actions	Processing Time	Person Responsible
1	*Client action:* Fill out the required information in the Incident Report Form/Technical Assistance Request Form. Submit all the accomplished forms together with all the relevant evidence such as log files, computer images, etc., through email. (cert-ph@dict.gov.ph). *Agency actions:* Receive and acknowledge the Incident Report Form and other supporting documents and for event verification, evaluation, and confirmation (Event VEC).	Within 1 day	Stakeholder
2	*Client action:* None. *Agency action:* The assigned analyst will process the submitted forms together with all the evidence provided by the stakeholder. These documents and artifacts will be verified and evaluated before considering it as an incident. Once the incident is confirmed through Event VEC, the assigned analyst will assign a ticket number and will start documenting all the important information about the incident.	Within 1 business day	CERT-PH Incident Responder/ Analyst
3	*Client action:* None. *Agency action:* The associated team will now perform its initial investigation to determine the incidents' scope such as which networks, systems, or applications are affected; who or what originated the incident; and how an incident is occurring. The assigned analyst will provide the agency a definite amount of time depending on the severity of the incident for the priority agency to address the incident and come up with an incident report. The assigned analyst may request additional evidence and information from the affected stakeholder or agency that may also help with the investigation.	Within 5 business days	CERT-PH Incident Responder/ Analyst
4	*Client action:* Submit all the requested additional information and evidence. *Agency action:* The assigned analyst will conduct further investigation and perform appropriate action once the requested additional information/evidence was already provided by the affected stakeholder.	Within 1 day	Stakeholder
5	*Client action:* None. *Agency action:* After the investigation, an incident response report is created by the assigned analyst. It includes all the information gathered by the incident responders as well as the process that they have performed and all the incident findings and recommendations. The incident response report will be submitted to the affected stakeholder for the remediation phase. Along with the process of creating an incident report the CERT-PH will schedule a debriefing meeting or conference call to discuss the lessons learned in relation to the incident.	Within 5 business days	CERT-PH Incident Responder/ Analyst

105 Adapted from Department of Information and Communications Technology, *Citizen's Charter*, 86–90.

Step	Required actions	Processing Time	Person Responsible
6	*Client action:* Once the affected stakeholder received the incident Response Report, followed the recommendations given by the assigned analyst and already remediated the incident, they should create an Action Taken Report which is to be submitted again to NCERT. Submit Action Taken Report through email. cert-ph@dict.gov.ph. *Agency action:* Receive the Action Taken Report from the affected stakeholder.	5 days	Stakeholder
7	*Client action:* None. *Agency action:* Once the assigned analyst received the Action Taken Report from the affected stakeholder, they will now close the ticket assigned to the incident and document all the details given in the Action Taken report.	Within 1 business days	CERT-PH Incident Responder/ Analyst
Total:		19 days	

Table 4. Cyber Threat Level Indicator.[106]

Color Indicator	Threat Level	Description	Report Timeframe
RED (rating 9–11)	Critical	Ransomware, C&C Server, DDOS affecting all critical sectors, data breach with critical information exposed, wide-spread destructive compromised system, 0-day, supply chain attacks	12 hours upon discovery of the incident
ORANGE (rating 6–8)	High	Compromised executive email, malware infiltration, network and system intrusion	18 hours upon discovery of the incident
YELLOW (rating 4–5)	Elevated	Detected known vulnerabilities, idle botnets and backdoors, unresolved signs of system intrusion (website defacements, etc.)	24 hours upon discovery of the incident
BLUE (rating 2–3)	Moderate	Phishing incidents, compromised systems/websites with non-sensitive information	48 hours upon discovery of the incident
Green (rating 0–1)	Low	Unverified anomalies	48 hours upon discovery of the incident

106 Adapted from Department of Information and Communications Technology National Computer Emergency Response Team, *CERT-PH Incident Reporting and Technical Assistance Request Guidelines*, 4–5.

Once an information security incident is detected, reported, and deemed relevant, the CERT-PH must conduct the response phase. During this phase, the CERT-PH conducts the containment protocol where they determine the cause of the incident and perform appropriate activities to immediately contain and minimize the impact. The containment activities include counteracting the immediate threat, preventing the expansion of the incident, minimizing potential damage, restricting "knowledge of the incident to authorized personnel," and preserving "information relevant to the incident."[107] Next, the CERT-PH determines and executes appropriate activities required to immediately secure and restore the processing environment or information system to an acceptable or operational state.[108] Moreover, the CERT-PH will actively be involved during the lifespan of the incident, "continuously assess the progress/status of all containment and corrective measures," and determine when the incident is "considered closed or resolved."[109] Figure 3 shows that in 2022, the CERT-PH handled 1,129 incidents, mostly malware and malicious files.

[107] Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, 13.

[108] Department of Information and Communications Technology, 14.

[109] Department of Information and Communications Technology, *DICT Computer Emergency Response Team (CERT) Manual*, 14.

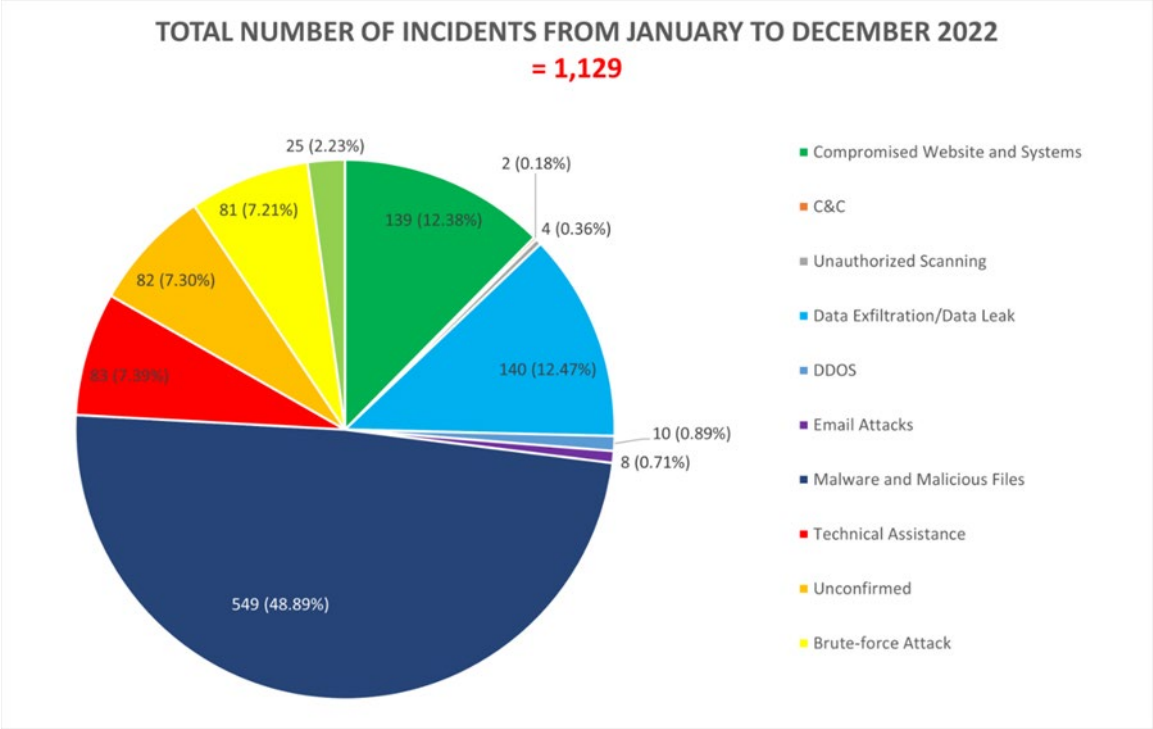

Figure 3. CERT-PH's Handled Incidents from January to December (2022).[110]

C. NATIONAL PRIVACY COMMISSION

1. Overview

The NPC is the Philippines' data privacy authority "committed to protect the personal information of data subjects and to foster a culture of privacy towards a competitive, knowledge-based, and innovative nation."[111] The NPC is assigned to "administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection."[112] Its mission is to provide "knowledge, know-how, and relevant technology;" "establish a regulatory environment that ensures accountability in the processing of personal data and

110 Source: "Total Number of Incidents from January to December 2022," GOVPH, accessed April 10, 2023, https://www.ncert.gov.ph/statistics/.

111 "About Us National Privacy Commission," National Privacy commission, accessed September 6, 2022, https://www.privacy.gov.ph/about-us/#quality_policy.

112 National Privacy commission, "About Us National Privacy Commission."

promotes global standards for data privacy and protection;" and "build a culture of privacy, through people empowerment, that enables and upholds the right to privacy and supports free flow of information."[113] The NPC provides various services such as data privacy resources, advisories, bulletins, journals, compliance information, and mechanics for complaints. Nevertheless, this chapter focuses on the NPC's data breach reporting process, administered under the Compliance and Monitoring Division and the Complaints and Investigation Division. Figure 4 displays the organizational chart for the NPC.

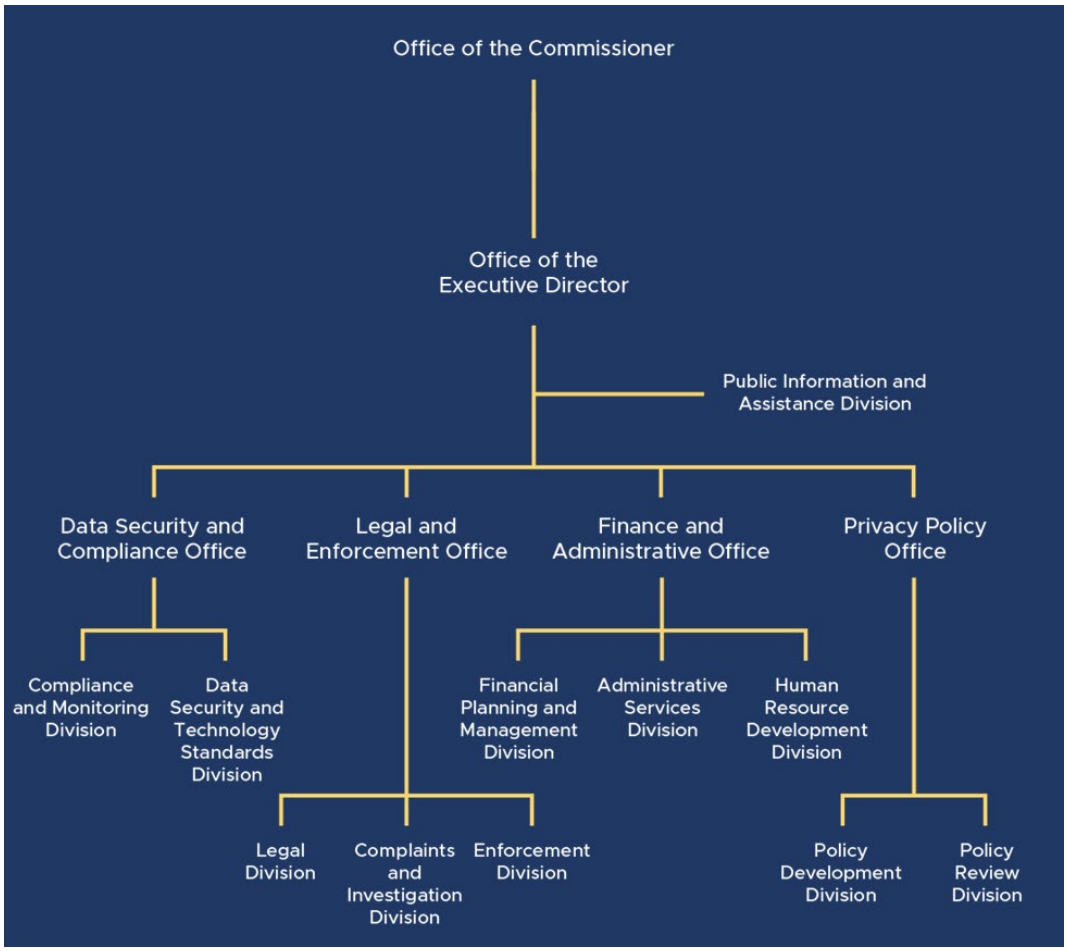

Figure 4. NPC's Organizational Chart.[114]

[113] National Privacy commission, "About Us National Privacy Commission."

[114] Source: National Privacy commission, "About Us National Privacy Commission."

2. Mandatory Data Breach Reporting

According to the NPC,

> A data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of or unauthorized processing of personal data. Compromises the availability, integrity, or confidentiality of personal data.[115]

A data breach must be reported to the NPC when "there is a breach of sensitive personal information" that enables identity fraud, reasonable belief unauthorized person acquired the data, and reasonable belief the data breach has the potential risk of serious harm to the affected data subjects.[116] The client's personal information controller or processor must submit a notification to the NPC within 72 hours, and a "full report of the personal data breach must be submitted within five (5) days from notification."[117] The data breach notification must include the following information: the nature of the breach, personal data involved, remedial measures, and name and contact details.[118]

Aside from notifying the NPC, the client's personal data controller must notify the affected data subjects within 72 hours through secure means of communication and should include the same content reported to the NPC, "instructions on how data subjects will receive further information," and "recommendations regarding how to minimize risks resulting from the breach."[119] The NPC can delay the notification requirement to the data subjects if the notification may hinder the progress of a criminal investigation.[120]

---

115 Vida Zora G. Bocar, "Breach Management and Reporting," National Privacy Commission, accessed September 19, 2022, https://www.privacy.gov.ph/wp-content/files/attachments/ppt/DPO5-BreachManagement.pdf.

116 "Exercising Breach Reporting Procedures," National Privacy Commission, accessed September 19, 2022, https://www.privacy.gov.ph/exercising-breach-reporting-procedures/.

117 National Privacy Commission, "Exercising Breach Reporting Procedures."

118 National Privacy Commission, "Exercising Breach Reporting Procedures."

119 National Privacy Commission, "Exercising Breach Reporting Procedures."

120 National Privacy Commission, "Exercising Breach Reporting Procedures."

Following the data breach, the NPC's Compliance and Monitoring Division assigns an evaluating officer to monitor the compliance of the personal information controller.[121] The evaluating officer considers the security measures implemented and applied during the data breach to include the personal information controller's "compliance with the law and existence of good faith in the collection of personal information."[122] Further, the division examines subsequent measures taken to minimize harm to the data subjects based on age and legal capacity, ensuring the notification of legal representatives for minors or those without legal capacity.[123] If applicable, the evaluating officer may request additional documents or apply for a cease and desist order.[124] Once all required information is received, the evaluating officer prepares a breach notification evaluation report to submit to the commission for adjudication.[125] However, if the findings require further investigation, the Compliance and Monitoring Division submits the report to the Complaints and Investigation Division (CID) instead.[126]

Upon receipt of a Breach Notification Evaluation Report, the CID assigns an investigating officer to conduct a technical or on-site investigation.[127] Depending on the nature of the incident, the investigation may include an "on-site examination of systems and procedures," "cooperation of concerned parties," "appropriate action therefrom to protect the interests of data subjects," and administration by "the Rules of Procedure of the Commission."[128] Upon the completion of the investigation or receipt of the breach notification evaluation report, the investigating officer submits a fact-finding report to the

---

121 National Privacy Commission, *2021 Rules of Procedures of the National Privacy Commission*, (Quezon City, Philippines: National Privacy Commission, 2021), 26–7, https://www.privacy.gov.ph/wp-content/uploads/2021/01/2021RULESOFPROCEDURE_VER8-Final-Sgd-1-1-1.pdf.

122 National Privacy Commission, "Exercising Breach Reporting Procedures."

123 National Privacy Commission, "Exercising Breach Reporting Procedures."

124 National Privacy Commission, 2021 Rules of Procedures of the National Privacy Commission, 27.

125 National Privacy Commission, 27.

126 National Privacy Commission, 27.

127 National Privacy Commission, 27.

128 National Privacy Commission, "Exercising Breach Reporting Procedures."

NPC within 30 days for adjudication.[129] Then, the commissioners conduct an adjudication meeting and release a decision, order, or resolution, which has a processing time of 19 days.[130] Last, the Compliance and Monitoring Division must monitor and ensure the client's personal information controller follows the commission's issued orders or resolutions.[131]

D. CYBERCRIME INVESTIGATION AND COORDINATING CENTER

1. Overview

Upon the approval of the Cybercrime Prevention Act of 2012, the CICC was created as an attached agency to the DICT for policy and program coordination. The CICC serves as the coordinating body for cybersecurity activities in the Philippines.[132] The CICC's mission is "to protect and secure the citizenry, country, and national sovereignty through effective institutional policies, programs and directives to prevent, suppress, and prosecute cybercrime."[133] The CICC has the power and function to formulate the National Cybersecurity Plan, establish the NCERT, monitor cybercrime cases handled by law enforcement and prosecution agencies, and coordinate the participation and support of local government units, non-government organizations, and the business sector in cybercrime prevention programs.[134] Moreover, the CICC facilitates international cooperation of intelligence, investigations, capacity building, and training related to

[129] National Privacy Commission, 2021 Rules of Procedures of the National Privacy Commission, 28.

[130] National Privacy Commission, *Citizen's Charter*, 1st ed. (Manila, Philippines: National Privacy Commission, 2021), 10, https://www.privacy.gov.ph/wp-content/uploads/2022/05/NPC-CITIZENS-CHARTER_1st-Edition.pdf.

[131] National Privacy Commission, 2021 Rules of Procedures of the National Privacy Commission, 28.

[132] Mamello Thinyane and Debora Christina, *Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies* (Macau: United Nations University, 2020), 56.

[133] CICC Cybercrime Investigation and Coordinating Center, *Citizen's Charter*, 1st ed. (Manila, Philippines: Cybercrime Investigation and Coordinating Center, 2021), 5, https://cicc.gov.ph/wp-content/uploads/2022/11/Final_CICC_Citizens-Charter_2021_June-29-July-2-11_03-AM.pdf.

[134] "Cybercrime Investigation and Coordinating Center (CICC)," GOVPH, accessed December 24, 2022, https://dict.gov.ph/cybercrime-investigation-and-coordinating-center-cicc/.

cybercrime prevention.[135] The CICC also recommends the enactment of appropriate cybersecurity measures and policies, laws, and issuances.[136] Although the CICC provides various functions, this chapter focuses on the CICC's process for submitting a request for a cybercrime investigation and cyber complaint, administered under the Investigation Division and the Digital Analytics Division. Figure 5 displays the organizational chart for the CICC.

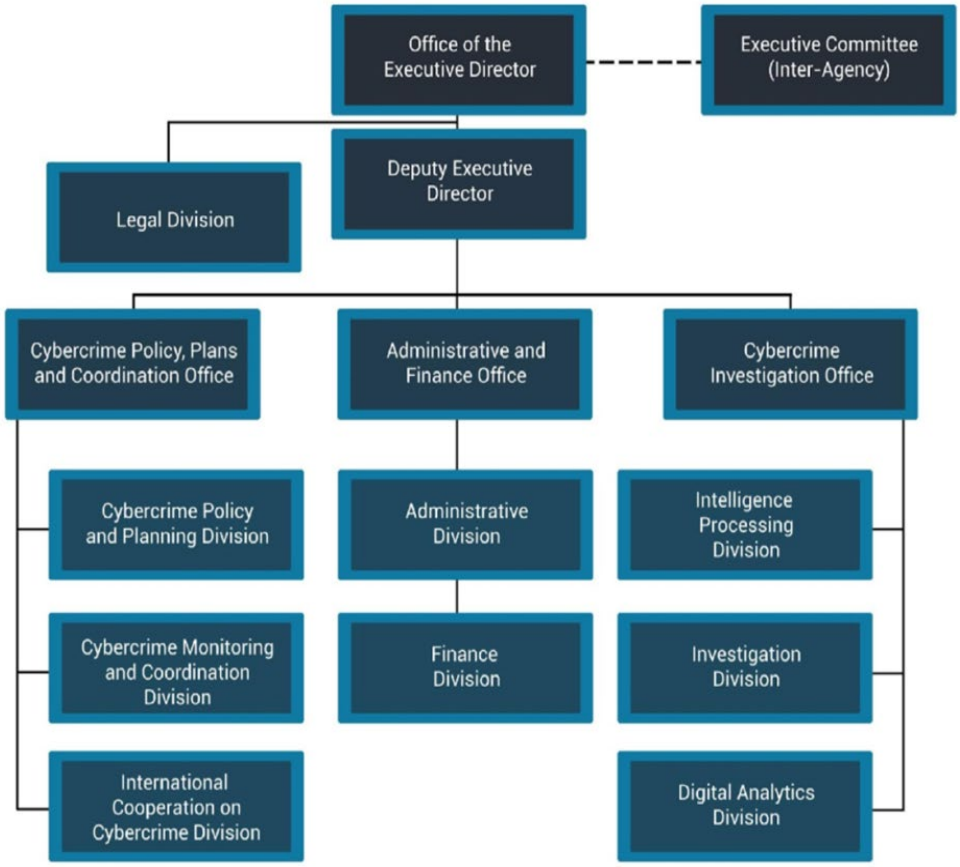

Figure 5. CICC's Organizational Chart.[137]

[135] GOVPH, "Cybercrime Investigation and Coordinating Center (CICC)."

[136] GOVPH, "Cybercrime Investigation and Coordinating Center (CICC)."

[137] Source: "About Us Organizational Chart," Cybercrime Investigation and Coordinating Center, accessed December 24, 2022, https://cicc.gov.ph/organizational-chart/.

2. Cybercrime Investigation

The CICC's Investigation Division is the lead unit on Cybercrime Investigation operations.[138] Thus, the Investigation Division may be directed or tasked to assist law enforcement agencies in investigating special cybercrime cases.[139] Additionally, concerned parties can submit a request for the conduct of a Cybercrime Investigation to the Investigation Division. Table 5 displays the step-by-step process to submit a request for the conduct of a Cybercrime Investigation.

Table 5. Request for the Conduct of Cybercrime Investigation.[140]

Step	Required actions	Processing Time	Person Responsible
1	*Client step:* Issue directive (Higher Office) or submit request (Other Concerned Parties) for the conduct of Cybercrime Investigation. *Agency actions:* 1.1. Acknowledge the receipt of the request, communication or directive and assign a tracking number.	3 working days	Receiving Officer, Investigation Division
	1.2. Case is assigned to an Investigation Officer who does an initial review of available documents and case facts.	1 working day	Investigation/Case Officer
	1.3. Conduct initial Coordinating/Case Conference with concerned CICC Officers/Personnel (Technical/Legal) to assess and determine next steps in moving forward with the case.	1 working day	Investigation/Case Officer
2	*Client step:* Collaborate with the CICC in the conduct of the investigation process. *Agency action:* 2.1. Work with the Requesting Party in gathering lacking documentary requirements and other relevant information (potential evidence).	3 working days	Investigation/Case Officer
	2.2 Based on initial findings, assigned CICC Case Officer shall conduct further investigation or case build-up with the assistance of the Technical/Legal Staff (CICC Investigation Team can be created as necessary).	3 working days	Investigation/Case Officer, Investigation Team
	2.3 Coordinate with Law Enforcement Units, other agencies/units of government (Court/LGU), and/or	3 working days	Investigation/Case Officer,

[138] CICC Cybercrime Investigation and Coordinating Center, Citizen's Charter, 11.

[139] CICC Cybercrime Investigation and Coordinating Center, Citizen's Charter, 11.

[140] Adapted from CICC Cybercrime Investigation and Coordinating Center, Citizen's Charter, 11–4.

Step	Required actions	Processing Time	Person Responsible
	concerned private companies (ISPs/Social Media Companies) for assistance, as needed. 2.4 Integrate and analyze gathered evidence and other relevant information to come up with case findings and recommendations. 2.5 Conduct final coordinating/case conference to present recommendations to concerned CICC authorities for guidance and approval (ED/DED/Director for Investigation Office).	 3 working days 2 working days	Investigation Team Investigation/Case Officer, Investigation Team Investigation/Case Officer, Investigation Team
3	*Client step:* Receive feedback or recommendation from CICC. *Agency action:* Transmit case findings/recommendations to Requesting Part, duly signed by authorized CICC Officers (ED/DED/Director for Investigation Office).	1 working day	Investigation/Case Officer
Total:		20 working days Note: In the assumption all documents/requirements needed are completed by clients.	

3. Cybercrime Complaint

The CICC's Digital Analytics Division is the lead unit on cyber complaints. Citizens can submit a cyber complaint to the Digital Analytics Division. Table 6 displays the process to submit a cyber complaint form.

Table 6. Submit a Cyber Complaint Form.[141]

Required actions	Processing Time	Person Responsible
Client step: Go to the website (https://cicc.gov.ph/filing-a-complaint/submit-a-cyber-complaint/) and provide all the necessary information on cybercrime and upload one (1) valid ID. *Agency actions:* 1. Staff receives and records cyber complaint form.	1 working day	Digital Analytics Division Staff
2. Collect, process and evaluate information.	3 working days	Digital Analytics Division Staff
3. Create initial report regarding the cyber complaint and forward it to the Intelligence and Investigation Division.	3 working days	Digital Analytics Division Staff
Total:	7 working days	

4. National Privacy Commission and Cybercrime Investigation and Coordinating Center Relationship

The NPC (established in 2016) and CICC (established in 2012) are attached agencies to the DICT that have different roles and functions, mandates, and jurisdictions. The NPC is primarily responsible for protecting personal data in the Philippines. It is tasked with implementing and enforcing the Data Privacy Act of 2012, which regulates the collection, use, processing, storage, and disposal of personal data by government agencies and private organizations. On the other hand, the CICC is responsible for coordinating and monitoring efforts to prevent, investigate, and prosecute cybercrime in the country. It works closely with law enforcement agencies and other government entities to address cyber threats and promote cybersecurity. The NPC focuses on protecting the privacy rights of individuals, while the CICC focuses on preventing and addressing cybercrime. The NPC and CICC may collaborate on matters related to data privacy and cybersecurity. For example, the NPC may provide technical assistance to the CICC in investigations involving personal data breaches. At the same time, the CICC may assist the NPC in identifying and addressing cyber threats to personal data. However, the two agencies maintain their

[141] Adapted from CICC Cybercrime Investigation and Coordinating Center, Citizen's Charter, 14–5.

separate mandates and do not interfere with each other's operations. They operate under different legal frameworks and have distinct powers and functions.

E. THE PHILIPPINES' CYBERSECURITY EFFORTS AND DEFICIENCIES

Through the DICT, CERT-PH, NPC, and CICC, the Philippine government has taken significant steps to establish effective cybersecurity measures and combat domestic and foreign cybercriminals. The functions of these agencies, described above, operate in a complementary fashion:

- The DICT formulates cybersecurity policies and programs to minimize cybercrime offenses and investigates cybercrime cases handled by law enforcement and prosecution agencies.
- The CERT-PH provides incident response services and technical assistance to government agencies, critical information infrastructure sectors, and other stakeholders.
- The NPC administers and implements the Data Privacy Act of 2012 and ensures compliance with international data protection standards. The NPC provides data privacy resources, advisories, and compliance information to prevent and address data breaches. It has established a data breach reporting process that requires timely notification and submission of reports by personal information controllers or processors. The NPC conducts investigations and releases decisions, orders, or resolutions to protect the interests of data subjects.
- The CICC facilitates international cooperation in intelligence, investigations, and capacity building. Its Investigation Division serves as the lead unit in cybercrime investigations, assisting law enforcement agencies in special cybercrime cases, and its Digital Analytics Division allows citizens to submit cyber complaints.

The establishment of the DICT, CERT-PH, NPC, and CICC, including their functions, reflect the Philippine government's commitment to cybersecurity, combatting and prosecuting domestic and foreign cybercriminals, and protecting cyberspace, critical infrastructure, and national security.

Despite the Philippines' progress in cybersecurity, a safe and secure cyberspace remains difficult to obtain. From 2017–2021, cyber threats detected in the Philippines have increased by 433%.[142] The Philippines encounters several challenges in the cybersecurity realm, including a reactive rather than proactive approach, initially low prioritization of cybersecurity concerns, digital transformation surpassing cybersecurity innovation, and stagnant budgets for cybersecurity despite rising cyber risks.[143] The Philippine government has limited capacity to patrol the cyber environment. Therefore, they have called for community participation to watch against malicious internet activity and provided online portals for citizens to submit cybersecurity incident reports.[144] The Philippine CERTs are not members of either the Forum of Incident Response and Security Teams or the Asia Pacific CERT organizations.[145] Based on the "Cisco 2018 Asia Pacific Security Capabilities Benchmark Study," the Philippines listed compatibility issues with legacy systems, reluctance to experiment with untested solutions, and, like many other countries, insufficient budget allocation as the top three reasons hindering the adoption of advanced security processes.[146]

Based on the functions of the DICT, CERT-PH, NPC, and CICC, there are a few areas that will likely offer the most promise for improvement in their cybersecurity efforts and ability to overcome cyber threats. The case studies in the following chapter probe these prospects in more detail. The remainder of this section outlines these possibilities, which

142 "PH 4th Among Countries Most Targeted by Web Threats," Philippines News Agency, February 21, 2022, https://www.pna.gov.ph/articles/1168257.

143 Castillo, "Philippine Cybersecurity in Retrospect (2016-2021)."

144 Thinyane and Christine, "Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies," 57.

145 Thinyane and Christine, 57.

146 Cisco 2018 Asia Pacific Security Capabilities Benchmark Study, 33.

include timeliness in incident and data breach reporting, the processing time for the NPC's decisions, orders, or resolutions, and conducting investigations.

Within the CERT-PH Division and NPC, there may be issues with the reporting and collection of incident reports and data breach reports. The CERT-PH Division relies on stakeholders to submit incident and data breach reports, while incidents and activities that do not necessarily affect the information system may not be reported. This may lead to underreporting of cybersecurity incidents and breaches, resulting in a lack of comprehensive data for effective analysis and response. Even though the CERT-PH Division and NPC set timeframes for reporting incidents and data breaches, there may be delays or gaps in reporting due to various factors, such as lack of awareness, fear of repercussions, or limited technical capabilities of stakeholders. Although the DICT provides external groups information, brochures, and materials about the CERT's purpose and services offered, it does not mean stakeholders are fully aware of the reporting requirements. In general, underreporting or delays in reporting cyber incidents and breaches may result in delayed or inadequate responses, containment, and resolutions, allowing cyber threats to persist and cause further damage.

While the CERT-PH Division and NPC are responsible for conducting containment activities, restoring the processing environment or information system to an operational state, and providing orders or resolutions, there may be challenges in ensuring timely and effective containment during the response phase. Depending on the cyberattack, the CERT-PH Division, NPC, and stakeholders may not have the necessary tools, capabilities, or access to quickly resolve a reported incident or data breach. The containment activities, such as counteracting immediate threats, preventing the expansion of the incident, and safeguarding information related to the incident, may require extensive technical expertise and resources. Further, monitoring and assessment require real-time analysis and evaluation of incidents and data breaches.

The effectiveness of prosecuting domestic and foreign cybercriminals depends on the proper implementation of laws, coordination among different agencies, and the capacity of law enforcement agencies to handle cybercrime cases. It is important to note that the effectiveness of the Philippine government's cybersecurity efforts and combatting

cybercriminals may be influenced by various factors, including the evolving nature of cyber threats, the level of cooperation from concerned parties, the capacity to enforce regulations and resource allocations. Cross-coordination and collaboration pose a challenge within the DICT, including its attached agencies, and between other stakeholders. Cybersecurity is a complex and evolving field, and effective response requires coordinating efforts among various government agencies, private sector organizations, and other stakeholders. Continuous efforts and improvements in cybersecurity policies, regulations, and issuances, fostering public-private partnerships, and promoting cybersecurity awareness among all stakeholders are crucial in addressing the evolving landscape of cyber threats and ensuring the effective prosecution of cybercriminals in the Philippines.

In conclusion, while the Philippines has made notable strides in tackling cybersecurity challenges, the effectiveness of its efforts remains uncertain. The Philippines has implemented more robust mandates to protect people's privacy and has taken additional steps to protect data privacy. The government has implemented legislation, developed cybersecurity plans, and established organizations to improve its cybersecurity capabilities. Through the DICT and the NPC, the Philippine government is well-positioned to disseminate recurring public information sharing on cyber threats and emphasize the necessity of devising an effective crisis management strategy in case of a cybersecurity breach.[147] As shown in this chapter, the Philippines has achieved positive results in its level of commitment to cybersecurity. Nonetheless, despite government mandates, procedures, and policies, ensuring compliance from stakeholders is not guaranteed, as effective cybersecurity requires cooperation from multiple parties and vigilant government oversight.

[147] Angel S. Averia et al., *Cybersecurity in the Philippines: Global Context and Local Challenges,* (San Francisco, CA: The Asia Foundation, 2022), 95, https://asiafoundation.org/publication/cybersecurity-in-the-philippines-global-context-and-local-challenges/.

F. SUMMARY OF REPORTING AND RESPONSE PROCEDURES

This chapter briefly overviews the DICT and its attached agencies: the NPC and the CICC. Furthermore, this chapter describes in detail the reporting and response procedures for cybersecurity incident reports, technical assistance request forms, data breach reporting, cybercrime investigation request forms, and cyber complaint forms.

Based on the information in this chapter, the Philippine government offers various services and reporting requirements via the DICT, NPC, and CICC that are readily available to organizations and citizens to deal with cyber threats. In principle, the Philippine government has the ability to overcome cyber threats and provide proper oversight to ensure organizations follow mandated government cybersecurity policies. But its performance in practice is less clear. Even though the Philippines has made significant progress in cybersecurity, there are several areas for improvement and it remains uncertain to how effective the progress has been. To provide a stronger basis for evaluating the Philippine government response overall, the following chapter investigates five important specific incidents in order to identify more specific shortcomings, opportunities for improvement, and the Philippine government's effectiveness in responding to cyberattacks.

III. ANALYSIS OF FIVE INCIDENTS OF CRITICAL CYBERATTACKS

A. INTRODUCTION

This chapter analyzes five incidents of critical cyberattacks that have occurred in the Philippines. These include the 2016 Commission on Election (COMELEC) government data breach, the 2017 Jollibee Foods Corporation (JFC) data breach, the 2018 Wendy's data breach, the 2019 Cebuana Lhuillier marketing server breach, and the 2021 LuminousMoth Advanced Persistent Threat (APT).[148] Four of the five incidents were listed as "the most serious data breach incidents in the ASEAN region during the past years."[149] One of the five, the 2021 LuminousMoth APT, was listed by the Center for Strategic and International Studies as the most recent significant cyber incident that targeted the Philippines.[150]

For each incident, the chapter attempts to answer the following sub-questions:

- Did the targeted organization report the cybercrime to the appropriate authorities?
- Did the Philippine government respond or provide any guidance to resolve the situation?
- If the Philippine government provided guidance, was it then followed?
- Was the problem resolved?
- Were the offenders identified? If so, who were they and what consequences did they face?

[148] An advanced persistent threat (APT) refers to a stealthy threat actor or group that illegally accesses a computer network and remains undetected for an extended period of time.

[149] Cristina Lago, "The Biggest Data Breaches in Southeast Asia," CIO, last modified January 18, 2020, https://www.cio.com/article/222022/the-biggest-data-breaches-in-the-asean-region.html.

[150] "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, 2022, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

The analysis of the incidents shows whether the Philippine government's responses to cyber threats have been effective and identifies deficiencies where those responses have fallen short. The information retrieved also determines how responsive targeted organizations were to cyberattacks to include following the Philippine government's guidance.

B. FIVE INCIDENTS OF CRITICAL CYBERATTACKS

1. The Philippine Commission on Election's 2016 Data Breach

From March 20–27, 2016, personal data was breached across several databases on the COMELEC website. The database included, "each voter's complete name, date of birth, gender, civil status, address, precinct number, birthplace, disability, voter identification number, voter registration record number, reason for deletion/deactivation, registration date, and update time."[151] The data breach affected 77,736,795 records, "making the incident the worst recorded breach on government-held personal database in the world, based on sheer volume."[152]

Two groups were allegedly involved in hacking the COMELEC website: Anonymous Philippines and LulzSec Pilipinas. Anonymous Philippines was known for defacing the website, while LulzSec Pilipinas publicly posted COMELEC's database via Facebook.[153] On April 21, 2016, the National Bureau of Investigation identified Paul Biteng as one of the suspected hackers in the group called Anonymous Philippines, and he admitted to defacing the COMELEC website.[154] On April 28, 2016, the National Bureau of Investigation tracked down Joenel de Asis as another suspected hacker in Anonymous

151 "Privacy Commission Recommends Criminal Prosecution of Bautista Over 'Comeleak'," Gov.PH, last modified November 11, 2021, https://www.privacy.gov.ph/2017/01/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/.

152 "Privacy Commission Recommends Criminal Prosecution of Bautista Over 'Comeleak'."

153 "Comelec Data Leaked by Hackers," Rappler, last modified March 28, 2016, https://www.rappler.com/nation/elections/127315-comelec-data-hackers/.

154 "NBI Resleases Suspected Comelec Hacker's Mugshot, GMA News Online," last modified April 21, 2016, https://www.gmanetwork.com/news/topstories/nation/563546/nbi-releases-suspected-comelec-hacker-s-mugshot/story/.

Philippines.[155] Joenel de Asis admitted to hacking the COMELEC website.[156] According to the National Bureau of Investigation Computer Crimes Division, Joenel de Asis also leaked COMELEC's database to the public under the name of the Lulz Security group.[157] Both members of Anonymous Philippines faced charges for violating the Cybercrime Prevention Act.[158]

On April 26, 2016, COMELEC submitted an initial report regarding the data breach to the NPC.[159] Aside from coordinating with the NPC, COMELEC worked with several other agencies, such as the National Bureau of Investigation, the Department of Justice, the Center for International Law Philippines, and the Department of Science and Technology's Information and Communications Technology Office, to help contain the situation. On December 28, 2016, the NPC recommended criminal prosecution of COMELEC's Chairman Juan Andres Bautista for violating "Sections 11, 20 and 21 of the Republic Act No. 10173."[160]

The NPC noted the data breach occurred due to the "lack of a clear data governance policy in COMELEC…website vulnerabilities…failure to monitor security breaches regularly."[161] As a corrective measure, the NPC ordered COMELEC to appoint a Data Protection Officer, conduct an agency-wide Privacy Impact Assessment, establish a breach management procedure and privacy management program, and implement security measures in accordance with the Data Privacy Act and NPC Circular 16–01 – Security of

---

155 Jamaine Punzalan, "NBI Arrests 2nd Hacker in Comelec Data Breach," ABS-CBN News, last modified April 29, 2016, https://news.abs-cbn.com/halalan2016/nation/04/29/16/nbi-arrests-2nd-hacker-in-comelec-data-breach.

156 Punzalan, "NBI Arrests 2nd Hacker in Comelec Data Breach."

157 Punzalan, "NBI Arrests 2nd Hacker in Comelec Data Breach."

158 Punzalan, "NBI Arrests 2nd Hacker in Comelec Data Breach."

159 RG Cruz, "Comelec to Report Data Leaks to Privacy Body," ABS-CBN News, last modified April 26, 2016, https://news.abs-cbn.com/halalan2016/nation/04/26/16/comelec-to-report-data-leaks-to-privacy-body.

160 "Privacy Commission Recommends Criminal Prosecution of Bautista Over 'Comeleak'."

161 Jamael Jacob and Jessamine Pacis, *"Revisiting the Breach: A Briefing Paper on the 2016 COMELEC Data Leak,"* (Quizon City, PH: Foundation for Media Alternatives, 2017), 7, https://www.fma.ph/wp-content/uploads/2018/04/COMELEAK-FINAL-1.pdf.

Personal Data in Government Agencies.[162] Since then, COMELEC has taken continuous measures to ensure compliance with the NPC and the Data Privacy Act.

Following are summary findings for COMELEC's data breach in terms of the five sub-questions posed in the chapter introduction:

- *Did the targeted organization report the cybercrime to the appropriate authorities?* Yes, upon the NPC's request, COMELEC submitted an initial report regarding the data breach to the NPC on April 26, 2016. This indicates COMELEC reported the cybercrime to the appropriate authorities. The incident was not reported within the 72-hour reporting requirement since the incident was identified on March 27, 2016. However, the 72-hour reporting requirement for cyber incidents may not have been a requirement until the release of NPC Circular 16–03 – Personal Data Breach Management on December 15, 2016.

- *Did the Philippine government respond or provide any guidance to resolve the situation?* Yes, the Philippine government responded to the situation by coordinating with various agencies, such as the National Bureau of Investigation, the Department of Justice, the Center for International Law Philippines, and the Department of Science and Technology's Information and Communications Technology Office, to help contain the situation. In addition, the NPC mandated COMELEC to appoint a Data Protection Officer, conduct a comprehensive Privacy Impact Assessment, establish a breach management procedure and privacy management program, and implement various security measures following the Data Privacy Act.

- *If the Philippine government provided guidance, was it then followed?* There was not enough information publicly released to determine the extent of COMELEC's cooperation with the NPC's guidance. However,

[162] "Privacy Commission Recommends Criminal Prosecution of Bautista Over 'Comeleak'."

COMELEC returned to normal operations, indicating COMELEC has complied with the NPC and Data Privacy Act.

- *Was the problem resolved?* Yes, several agencies worked together to resolve the incident while COMELEC took continuous measures to ensure compliance with the NPC and the Data Privacy Act.

- *Were the offenders identified? If so, who were they and what consequences did they face?* Yes, the offenders were identified. Two members of Anonymous Philippines, Paul Biteng and Joenel de Asis, were identified as suspected hackers involved in the data breach. Paul Biteng admitted to defacing the COMELEC website, and Joenel de Asis admitted to hacking the COMELEC website and leaking the database to the public. Both faced charges for violating the Cybercrime Prevention Act.

In summary, COMELEC submitted an incident report to the NPC upon request, even though it was not within the 72-hour reporting requirement. Various government agencies, including COMELEC, were able to work together to contain the situation, ensure COMELEC's compliance with the NPC and Data Privacy Act, and identify the offenders. As a result, the Philippine government and COMELEC are determined to have effectively responded to the COMELEC data breach.

2. Jollibee Foods Corporation's 2017 Data Breach

On December 12, 2017, JFC informed the NPC that persons unknown were able to breach Jollibee's delivery website on December 8, 2017.[163] During an investigation, the CID identified that a domestic cybersecurity firm conducted the breach during a proof-of-concept activity initiated by a Jollibee marketing public relations team representative. Although the cybersecurity firm detected a security gap within the jollibeedelivery.com website and "were able to exploit the vulnerabilities, their firm insisted that they did not scrape or exfiltrate any data, because they merely demonstrated their ability to access the

[163] CIDBN No. 17-043, 1 (2018), https://www.privacy.gov.ph/wp-content/files/pospp/CIDBN_17-043_ORDER_May042018.pdf.

data in Jollibee's database if they so desired."[164] JFC's Data Protection Officer, J'Mabelard Gustilo, decided to "handle corrective measures internally and through its third party IT security provider."[165] He clarified that the "JFC Group treated the cybersecurity firm responsible for the breach as an uncontracted entity or stranger who had no authority to infiltrate their IT infrastructure."[166]

In a later meeting, CID noticed some improvements in Jollibee's database protection, but more efforts were needed to protect the data.[167] On February 20, 2018, the CID conducted a vulnerability assessment of Jollibee's delivery website and identified that its online properties were vulnerable to unauthorized access,[168] putting 18 million customers on the database at "very high risk."[169] Thus, on May 4, 2018, under Order CIDBN 17-043, JFC was ordered to conduct the following actions:

1. **SUSPEND** forthwith the operations of jollibeedelivery.com and all other data processing open to the public through the internet and restrict external access to their networks, for an indefinite time until the site's identified vulnerabilities are addressed, as validated by a duly certified penetration testing methodology.
2. **SUBMIT** a security plan to be implemented in rehabilitating said system to ensure the integrity and retention of the database and its content within ten (10) calendar days upon receipt hereof.
3. **EMPLOY** Privacy by Design in the reengineering of JFC Group data infrastructure.
4. **CONDUCT** a new Privacy Impact Assessment, considering the vulnerabilities exposed in the Commission's penetration tests and in subsequent penetration tests ordered in the next preceding section.
5. **FILE** a monthly Progress Report on this matter until the issues raised in this Order are resolved.[170]

---

[164] CIDBN No. 17-043.

[165] CIDBN No. 17-043.

[166] CIDBN No. 17-043.

[167] CIDBN No. 17-043.

[168] CIDBN No. 17-043.

[169] "Philippine Privacy Regulator Suspends Jollibee's Online Delivery Site," S&P Global, last modified May 7, 2018, https://www.spglobal.com/marketintelligence/en/news-insights/trending/yjT6xL9pGN5rP4OOIlgaBA2.

[170] CIDBN No. 17-043.

Following Order CIDBN No. 17-043, Jollibee's delivery website was shut down and suspended "for an indefinite time until the site's identified vulnerabilities are addressed, as validated by a duly certified penetration testing methodology."[171] JFC stated, "We are currently addressing the issues the [NPC] has outlined, and we are closely coordinating with them on this."[172] Privacy Commissioner Raymund Liboro later stated, "Jollibee is on the road to compliance."[173] The website was later restored, indicating a sufficient level of responsiveness.

Following are summary findings for JFC's data breach in terms of the five sub-questions posed in the chapter introduction:

- *Did the targeted organization report the cybercrime to the appropriate authorities?* Yes, JFC submitted an initial report regarding the data breach to the NPC on December 12, 2017, indicating JFC reported the cybercrime to the appropriate authorities. The incident was not reported within the 72-hour reporting requirement: the incident occurred on December 8, 2017.

- *Did the Philippine government respond or provide any guidance to resolve the situation?* Yes, the CID responded to the situation by establishing Order CIDBN 17-043 on May 4, 2018. However, this was five months after the incident. Before the order, the CID enabled JFC to handle corrective measures internally until the CID discovered JFC's online properties were still vulnerable to unauthorized access during a vulnerability assessment on February 20, 2018.

171 CNN Philippines Staff, "Wendy's PH Website Hack Exposes Thousands of Personal Data," CNN, last modified May 9, 2018, https://www.cnnphilippines.com/business/2018/05/08/wendys-jollibee-website-hack-delivery.html.

172 Gelo Gonzales, "Jollibee Deliver website Suspended Over 'Serious Vulnerabilities'," Rappler, last modified May 8, 2018, https://www.rappler.com/technology/202061-national-privacy-commission-jollibee-delivery-website-suspension/.

173 Bernie Cahiles-Magkilat, "NPC to Render Decision on Facebook Data Breach," Manila Bulletin, last modified August 18, 2018, https://mb.com.ph/2018/08/18/npc-to-render-decision-on-facebook-data-breach/.

- *If the Philippine government provided guidance, was it then followed?* There was not enough information publicly released to determine the extent of JFC's cooperation with the CID. Privacy Commissioner Raymund Liboro's statement, "Jollibee is on the road to compliance,"[174] indicates Jollibee was implementing the CID's guidance.

- *Was the problem resolved?* JFC's website was shut down indefinitely until vulnerabilities were addressed. However, since the website is currently up and running, it is assumed that JFC followed the guidance provided and the problem was resolved in order for JFC to continue its online operations.

- *Were the offenders identified? If so, who were they and what consequences did they face?* Yes, the offenders were identified. A domestic cybersecurity firm conducted the breach during a proof-of-concept activity initiated by a Jollibee marketing public relations team representative. JFC treated the cybersecurity firm responsible for the breach as an uncontracted entity or stranger with no authority to infiltrate its IT infrastructure. It is not known publicly if the cybersecurity firm faced any consequences.

In summary, JFC submitted an initial report to the NPC four days after the incident was identified, failing to meet the 72-hour reporting requirement. The CID enabled JFC to handle the incident internally and did not serve an order to JFC until five months after the incident. Although the problem was presumed resolved and the offenders were identified, JFC and the Philippine government's responses were delayed. As a result, JFC and the Philippine government's responses to the data breach are determined to have been ineffective.

[174] Bernie Cahiles-Magkilat, "NPC to Render Decision on Facebook Data Breach," Manila Bulletin, last modified August 18, 2018, https://mb.com.ph/2018/08/18/npc-to-render-decision-on-facebook-data-breach/.

3. Wendy's Philippine 2018 Data Breach

On April 23, 2018, attackers breached Wendy's Philippine website and took names, contact numbers, emails, addresses, and résumés, affecting roughly 82,150 records.[175] The NPC issued Order CIDBN No. 18-058 to Wendy's restaurant, Inc. "in relation to the data breach affecting Wenphil Corporation ("Wendy's") on 23 April 2018."[176] The order stated, "On 23 April 2018, yet unknown persons published online a database containing the Wendy's Philippine website in its entirely."[177] It further mentioned that Wendy's Philippines notified the NPC on April 26, 2018 that their website was infiltrated and personal data was exfiltrated, asserting that the exposure of such data put data subjects at risk of serious harm.[178] In addition, the breach required Wendy's to adequately notify the affected data subjects. However, on May 2, 2018, during a meeting between representatives from Wendy's and the NPC, it was recognized that Wendy's did not "inform the affected data subjects of the note, scope, and extent of the breach, notwithstanding the clear mandate of NPS Circular No. 16–03 on breach notifications, and the contents thereof."[179] Thus, on May 2, 2018, under Order CIDBN No. 18-058, Wendy's was ordered to perform the following actions:

1. **NOTIFY** all affected data subjects with exposed sensitive personal information or information that can be used to enable identity fraud, pursuant to the requirements contained within NPC Circular No. 16–03 within 72 hours from the issuance of this Order;
2. **EXPLAIN** to this Commission why further action should not be taken against Wenphil Corporation for their failure to notify the affected data subjects within the proper period required in NPC Circular No. 16–03.
3. **PROVIDE** a copy of Server Logs, Network Logs, and Traffic Logs of the https://wendys.com.ph website prior to the breach;
4. **SUBMIT** the updated version of the applicable Privacy Policy in force at the time of the data breach, an update of the internal investigation

175 "Wendy's PH Informs Users of Site Data Breach after NPC Intervention," Rappler, last modified May 8, 2018, https://www.rappler.com/technology/202040-wendys-philippines-data-breach/.

176 CIDBN No. 18-058, 1 (2018), https://www.privacy.gov.ph/wp-content/files/pospp/CIDBN_18-058_ORDER_May022018.pdf.

177 CIDBN No. 18-058.

178 CIDBN No. 18-058.

179 CIDBN No. 18-058.

conducted, and the policy on transaction procedures, and any and all prior recommendations for information security measures that were not implemented.

5. **CONDUCT** a new Privacy Impact Assessment, taking into account the vulnerabilities exposed in this latest data breach.[180]

Following Order CIDBN No. 18-058, Wendy's did notify affected data subjects of the security breach via text message stating,

> [Wendy's] would like to inform [data subjects] that there has been a security breach on Wendy's PH website. Personal data provided in [Wendy's] website particularly [data subjects] name, email address, contact number, address, and [data subjects] resume might have been compromised. Wendy's website has already been shut down and we are currently conducting investigation on the incident. [Wendy's] are coordinating with the NPC, [Wendy's] host provider and payment gateway for immediate action to prevent damage to [Wendy's] data subjects.[181]

At the time of the incident, the wendys.com.ph website was shut down[182] but later became active again, displaying an updated data privacy policy that required users to agree before proceeding onto the website. According to Privacy Commissioner Raymund Liboro, "[Jollibee and Wendy's] have been complying with their compliance orders."[183]

Following are summary findings for Wendy's data breach in terms of the five sub-questions posed in the chapter introduction:

- *Did the targeted organization report the cybercrime to the appropriate authorities?* Yes, Wendy's Philippines notified the NPC about the data breach on April 26, 2018, which was three days after the incident occurred.

---

180 CIDBN No. 18-058.

181 "Wendy's PH Informs Users of Site Data Breach after NPC Intervention."

182 CNN Philippines Staff, "Wendy's PH Website Hack Exposes Thousands of Personal Data," CNN, last modified May 9, 2018, https://www.cnnphilippines.com/business/2018/05/08/wendys-jollibee-website-hack-delivery.html.

183 Bernie Cahiles-Magkilat, "NPC to Render Decision on Facebook Data Breach," Manila Bulletin, last modified August 18, 2018, https://mb.com.ph/2018/08/18/npc-to-render-decision-on-facebook-data-breach/.

- *Did the Philippine government respond or provide any guidance to resolve the situation?* Yes, the NPC issued Order CIDBN No. 18-058 to Wendy's concerning the data breach affecting Wenphil Corporation on April 23, 2018.

- *If the Philippine government provided guidance, was it then followed?* The guidance was not followed to its full extent. On April 26, 2018, Wendy's was ordered to notify the affected subjects. Still, Wendy's did not notify them until after NPC issued Order CIDBN No. 18-058 stating on May 2. There is a lack of public information or announcements to determine if Wendy's complied with the rest of the guidance stated in Order CIDBN No. 18-058 other than Privacy Commissioner Raymund Liboro stating, "[Jollibee and Wendy's] have been complying with their compliance orders."[184]

- *Was the problem resolved?* Wendy's website was shut down but became active with an updated data privacy policy. Since the website is currently up and running, it is assumed that Wendy's followed the guidance provided, and the problem was resolved for Wendy's to continue its online operations.

- *Were the offenders identified? If so, who were they and what consequences did they face?* This research did not identify information that mentioned whether offenders behind the data breach were identified or faced any consequences.

In summary, Wendy's submitted an initial report to the NPC three days after the incident was identified, meeting the 72-hour reporting requirement. However, Wendy's did not notify affected subjects after the NPC told it to do so on April 26, 2018. A week after

[184] Bernie Cahiles-Magkilat, "NPC to Render Decision on Facebook Data Breach," Manila Bulletin, last modified August 18, 2018, https://mb.com.ph/2018/08/18/npc-to-render-decision-on-facebook-data-breach/.

submitting the initial report, the NPC issued Order CIDBN No. 18-058 to Wendy's. Presumably Wendy's followed the order and the problem was resolved, but the offenders were not identified. As a result, Wendy's response to the data breach is determined to have been ineffective, while the Philippine government's response is determined to have been effective.

4. Cebuana Lhuillier's 2019 Data Breach

On January 15, 2019, Cebuana Lhullier—a Philippine based pawnshop—detected a data breach that affected 900,000 customers, leaking sources of income, birthdays, and addresses.[185] During the confirmation of the breach, Cebuana Lhuillier's affected server was immediately disconnected from the network[186] and the breach was reported to the NPC.[187] Privacy Commissioner, Raymond Liboro, confirmed Cebuana Lhuiller notified the NPC and requested assistance regarding the data breach.[188] According to Raymond Liboro, Cebuana Lhullier had 72 hours from detection of the data breach to notify affected data subjects.[189] He further confirmed the incident was under investigation.[190]

Cebuana Lhullier notified clients via email, stating,

> We are writing to inform you of a security incident which may have affected your personal data stored in one of our email marketing tool servers. On January 15, 2019, we detected attempts to use one of our email servers as a relay to send out spam to other domains. Follow-up investigation resulted in the discovery of

185 Luis Medillo, "Cebuana Lhuillier Data Breach Affects 900,000 Customers," Tech Pilipinas, last modified January 19, 2019, https://techpilipinas.com/cebuana-lhuillier-data-breach/.

186 Medillo, "Cebuana Lhuillier Data Breach Affects 900,000 Customers."

187 Katrina Domingo, "Cebuana Lhuillier Bares Data Breach, Tells Clients to Secure Accounts," ABS-CBN News, last modified January 19, 2019, https://news.abs-cbn.com/business/01/19/19/cebuana-lhuillier-bares-data-breach-tells-clients-to-secure-accounts.

188 "Official Statement of Privacy Commissioner Raymund Enriquez Liboro on the Cebuana Lhuiller Breach," GovPH, last modified November 11, 2021, https://www.privacy.gov.ph/2019/01/official-statement-of-privacy-commissioner-raymund-enriquez-liboro-on-the-cebuana-lhuiller-breach/.

189 "Official Statement of Privacy Commissioner Raymund Enriquez Liboro on the Cebuana Lhuiller Breach."

190 "Official Statement of Privacy Commissioner Raymund Enriquez Liboro on the Cebuana Lhuiller Breach."

> unauthorized downloading of contact lists used as recipients for email campaigns. These unauthorized downloads took place on August 5, 8, and 12, 2018.[191]

The email also provided affected users with precautionary measures and steps to protect their information.[192] In addition, Cebuana Lhullier released an official statement,

> Upon discovery, we immediately coordinated with the National Privacy Commission (NPC) to investigate the matter, and already implemented safety measures to protect the personal data of our clients. We also notified all affected clients and provided them guidance on how to further protect their personal information.[193]

According to the Bangko Sentral ng Pilipinas, the central bank of the Philippines, Cebuana Lhuillier's data breach incident was contained as the main servers were not affected, transaction details were safe, and the Bangko Sentral ng Pilipinas closely monitored the situation.[194]

Following are summary findings for Cebuana Lhuillier's data breach in terms of the five sub-questions posed in the chapter introduction:

- *Did the targeted organization report the cybercrime to the appropriate authorities?* Yes, Cebuana Lhuillier notified the NPC about the data breach, but public information did not state when the NPC was notified. Therefore, it is unknown if Cebuana Lhullier met the 72-hour reporting requirement.

- *Did the Philippine government respond or provide any guidance to resolve the situation?* Yes, the NPC informed Cebuana Lhuillier it had 72 hours to inform affected subjects. Further, the NPC investigated the matter

191 Medillo, "Cebuana Lhuillier Data Breach Affects 900,000 Customers."

192 "Cebuana Lhuillier Confirmed Hacked in Their Database," Litrato Philippines, last modified January 19, 2019, https://litratopilipinas.wordpress.com/2019/01/19/cebuana-lhuillier-confirmed-hacked-of-their-database/.

193 Medillo, "Cebuana Lhuillier Data Breach Affects 900,000 Customers."

194 Melissa Lopez, "BSP Says Cebuana Lhuillier Data Breach 'Contained'," BusinessWorld Publishing, last modified January 28, 2019, https://www.bworldonline.com/banking-finance/2019/01/28/210934/bsp-says-cebuana-lhuillier-data-breach-contained/.

and coordinated with Cebuana Lhuillier on the issue. However, there was a lack of public information stating the kind of guidance the NPC provided, and there was not a CID order readily available for this incident.

- *If the Philippine government provided guidance, was it then followed?* Yes, based on the limited information available, Cebuana Lhuillier notified all affected subjects and guided them on further protecting their personal information. This suggests the guidance provided by the Philippine government was followed.

- *Was the problem resolved?* Yes, the incident was contained as the main servers were not affected, and transaction details were safe. Steps were taken to address the issue and mitigate further damage.

- *Were the offenders identified? If so, who were they and what consequences did they face?* The research did not identify information that mentioned whether offenders behind the data breach were identified or faced any consequences.

In summary, Cebuana Lhuillier notified the NPC and the affected subjects of the data breach. The NPC investigated the matter, coordinated with Cebuana Lhuillier, and contained the incident. Although offenders were not identified, based on the actions taken and the outcome of the incident, Cebuana Lhuillier and the Philippine government's response to the data breach is determined to have been effective.

5. 2021's LuminousMoth Advanced Persistent Threat

On July 14, 2021, Kaspersky—a global cybersecurity company headquartered in Moscow, Russia—announced that its experts identified a wide-ranging APT campaign that targeted 1,400 users in the Philippines, including government entities.[195] These APT activities—nicknamed LuminousMoth—were attributed to the Chinese-speaking threat

195 "Rare, Mass Advanced Threat Campaign Targets More Than a Thousand Users in Southeast Asia," Kaspersky, July 14, 2021, https://www.kaspersky.com/about/press-releases/2021_rare-mass-advanced-threat-campaign-targets-more-than-a-thousand-users-in-southeast-asia.

actor, the HoneyMyte—a threat group involved in retrieving economic and geopolitical intelligence in Asia and Africa.[196] Although the APT campaign was discovered in July 2021, according to Kaspersky, LuminousMoth "has been conducting cyberespionage attacks against government entities since at least October 2020."[197] The APT used spear-phishing emails containing a Dropbox download tied to a malicious Word document.[198] Once downloaded, the malware was capable of spreading to other servers via removable USB drives.[199] The APT contained two post-exploitation tools: a fake version of Zoom (a software signed by a Shanghai organization) and a tool that stole Chrome user-authentication cookies.[200] In turn, the APT exfiltrated data and sensitive information to the attacker's command-and-control infrastructure.[201] The cookies stolen were dedicated to hijacking and impersonating Gmail sessions of the victims.[202]

On July 15, 2021, the CERT-PH posted information about the APT Group on its Facebook page and website, which included a description of the attack, actions to be taken, and a list of indicators of compromise. The CERT-PH recommended the following action to potential victims:

- Check systems and devices for known vulnerabilities, and if applicable, apply the necessary patches and updates to mitigate security threats.
- It is highly advised to check for any indicators of compromise, such as suspicious files and unusual external communication. (Please see [the list of indicators of compromise] for reference.)

196 "Rare, Mass Advanced Threat Campaign."

197 "Rare, Mass Advanced Threat Campaign."

198 "Rare, Mass Advanced Threat Campaign."

199 "Rare, Mass Advanced Threat Campaign."

200 "Rare, Mass Advanced Threat Campaign Targets More Than a Thousand Users in Southeast Asia."; Lisa Vaas, "Fake Zoom App Dropped by New APT 'LuminousMoth'," Threatpost, last modified July 15, 2021, https://threatpost.com/zoom-apt-luminous-moth/167822/.

201 "Rare, Mass Advanced Threat Campaign Targets More Than a Thousand Users in Southeast Asia.": "Advanced Persistent Threat Group LuminousMoth Targeting Government Organization from the Philippines," GOVPH, last modified July 15, 2021, https://www.ncert.gov.ph/2021/07/15/advanced-persistent-threat-group-luminousmoth-targeting-government-organizations-from-the-philippines/.

202 Charlie Osborne, "Chinese APT LuminousMoth Abuses Zoom Brand to Target Gov't Agencies," ZDNET, last modified July 16, 2021, https://www.zdnet.com/article/chinese-apt-luminousmoth-abuses-zoom-brand-to-target-govt-agencies/.

- Proactively monitor and secure systems and devices for any suspicious/ malicious activities.
- Secure and ensure backups of critical data are always available and can be deployed, if an incident will occur.
- Provide employees with ample knowledge and training with regards to good cyber hygiene practices.[203]

It is unknown whether any Philippine entities came forward to report LuminousMoth attacks. It is also unknown if personnel or entities followed CERT-PH's recommended actions and if the problem was resolved. Moreover, information has yet to be released that has declared LuminousMoth a continued problem since its discovery in July 2021.

Summary of LuminousMoth APT findings:

- *Did the targeted organization report the cybercrime to the appropriate authorities?* Based on the information provided, it is unclear whether the targeted organizations affected by the LuminousMoth APT campaign in the Philippines reported the cybercrime to the CERT-PH or appropriate authorities.

- *Did the Philippine government respond or provide any guidance to resolve the situation?* The CERT-PH responded and guided potential victims of the LuminousMoth APT campaign. The CERT-PH posted information on its Facebook page and website, which included a description of the attack and recommended actions to be taken, such as checking systems for vulnerabilities, monitoring for suspicious activities, securing backups of critical data, and providing employees with cybersecurity training.

203 "Advanced Persistent Threat Group LuminousMoth Targeting Government Organization from the Philippines."

- *If the Philippine government provided guidance, was it then followed?* It is unknown if affected personnel or entities of the LuminousMoth APT campaign followed the CERT-PH's recommended actions.

- *Was the problem resolved?* Based on the limited information discovered, it is unknown whether the LuminousMoth APT campaign was resolved since its discovery in July 2021 or if the APT group is still active.

- *Were the offenders identified? If so, who were they and what consequences did they face?* The information provided attributes the LuminousMoth APT campaign to the HoneyMyte threat group, which is described as a Chinese-speaking threat actor involved in retrieving economic and geopolitical intelligence in Asia and Africa. However, there is no information available to determine if the offenders were specifically identified or if they faced any consequences.

In summary, it is unknown whether targeted organizations came forward to report cyber incidents related to the LuminousMoth APT. Although the CERT-PH responded and provided guidance to potential victims of the LuminousMoth APT campaign on its Facebook page and website, the information was limited and it is unknown whether affected personnel followed the guidance. Further, it is unknown if the LuminousMoth APT was contained or resolved and if offenders were identified. As a result, it is difficult to determine whether the Philippine government's response to the APT was effective.

C. SUMMARY OF THE FIVE INCIDENTS OF CRITICAL CYBERATTACKS

This chapter analyzed five incidents of critical cyberattacks. Table 7 displays a summary of the five incidents of critical cyberattacks in terms of the five metrics applied in the preceding discussion.

Table 7. Table Summary of the Five Incidents of Critical Cyberattacks.

	COMELEC (2016)	Jollibee (2017)	Wendy's (2018)	Cebuana (2019)	LuminousMoth (2021)
Cybercrime Reporting	Yes	Yes	Yes	Yes	Unknown
Philippine government response	Yes	Yes	Yes	Yes	Yes
Guidance followed	Yes	Yes	Yes	Yes	Unknown
Problem resolved	Yes	Yes	Yes	Yes	Unknown
Offenders identified	Yes	Yes	No	No	No
Summary: Philippine gov't effective	Yes	No	Yes	Yes	Unclear

In conclusion, the findings of the data breaches at COMELEC, JFC, Wendy's, and Cebuana Lhuillier in the Philippines indicate that the targeted organizations reported the cybercrimes to the appropriate authorities. Still, COMELEC and JFC did not report the incidents within the 72-hour reporting requirement window, and it was unknown if Cebuana Lhuillier met the timeline. In these four cases, the Philippine government responded and provided guidance to resolve the situation. However, there was a lack of public information regarding the full extent of compliance with the guidance provided. The research showed a delay in compliance with government guidance for the Wendy's case since it failed to notify the affected subjects when directed on April 23, 2018. Based on these four cases and the limited information available, the problems were resolved as the organizations took measures to address the vulnerabilities, improve their data privacy practices, and maintain current operations.

In reference to the LuminousMoth APT, it is unclear whether the targeted organizations affected reported the incident to the appropriate authorities. CERT-PH did post information on its Facebook page and website, describing the attack and recommending actions to be taken. However, it is unknown if affected personnel or entities followed CERT-PH's recommended actions. Further, it is unknown whether the LuminousMoth APT campaign was resolved since its discovery in July 2021 or if the APT group is still active. For all five cases, offenders were only identified in the COMELEC and JFC cases, while the consequences the offenders faced were unknown to the public.

The Philippine government responded to the five incidents, but its level of effectiveness has mixed results for each case. The Philippine government was determined to have been effective during the COMELEC, Wendy's, and Cebuana Lhuillier cases, but ineffective during the JFC case. Based on the limited information retrieved from the LuminousMoth APT, it was undetermined whether the Philippine government responded effectively. For the most part, the Philippine government lacked the ability to identify offenders and hold them accountable for their actions.

Next, the targeted organizations' level of effectiveness in response to the cyber incidents and compliance with the Philippine government's guidance also had mixed results. COMELEC and Cebuana Lhuillier's responses to their respective cyber incident were determined to be effective. On the other hand, JFC and Wendy's were ineffective in their response to their respective cyber incidents. Regarding the LuminousMoth APT, it was unknown to which organizations were targeted and affected by the APT.

Taking all these elements into consideration, a further observation emerges: the responses of government agencies were reactive rather than proactive in dealing with cybersecurity issues. This was noticed when the Philippine government relied on targeted organizations to report cyber incidents, resulting in delays. The Philippine government has policies and procedures to help resolve cyberattacks after a breach has occurred. However, the policies lacked adequate security measures, such as continuous monitoring and enforcement mechanisms, to prevent cyberattacks from occurring. Like any other country, the Philippines continues to face cybersecurity challenges that require policies to be consistently assessed and updated to keep up with the evolving cyber threats.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

This thesis sought to answer the following research question: How effective has the Philippine government been in addressing cyber threats within its country? To answer the research question, this thesis evaluated the Philippine government's laws, processes, and procedures as well as five major historical cyberattack cases: the 2016 Commission on Election (COMELEC) data breach, the 2017 Jollibee Foods Cooperation (JFC) data breach, the 2018 Wendy's data breach, the 2019 Cebuana Lhuillier data breach, and the 2021 LuminousMoth Advanced Persistent Threat (APT). The research findings provide insight into the Philippine government's ability to respond to cyber threats. Moreover, this thesis examined pertinent literature and empirical evidence to add to the debate on whether the government responds effectively. This chapter discusses findings and policy using information provided in chapters I, II, and III. Lastly, this chapter provides research limitations and areas for further research to provide additional insights to further analyze the Philippine government's effectiveness in addressing cyber threats within its country.

A. FINDINGS

Like the literature review, chapters II and III confirm that the Philippine government has implemented several policies and programs to improve cybersecurity. Through the Department of Information and Communications Technology (DICT), Computer Emergency Response Team Philippines (CERT-PH), National Privacy Commission (NPC), and Cybercrime Investigation and Coordinating Center (CICC), the Philippine government has taken significant steps to establish cybersecurity measures and combat domestic and foreign cybercriminals, while challenges remain. This thesis adds to the debate mentioned in the literature review of whether these policies have been adequately enforced or benefitted the Philippines.

Chapter II shows the NPC has established a data breach reporting process that requires timely notification and submission of reports while highlighting potential delays or gaps in reporting incidents and data breaches. In Chapter III, these reporting delays were identified when COMELEC and JFC failed to report their respective data breaches to the

NPC within the 72-hour timeframe. At the same time, it was unclear if Cebuana Lhuillier met the timeline. According to the NPC, not only are data breaches supposed to be reported within 72 hours when there is a breach of sensitive personal information that enables identity fraud, but affected data subjects are to be notified within 72 hours through secure means of communication. As Chapter III states, Wendy's failed to notify affected subjects within the allotted timeframe. Chapter II mentions potential issues in underreporting cybersecurity incidents and breaches, contributing to a lack of comprehensive data for effective analysis and response. In Chapter III, underreporting was a plausible issue regarding the LuminousMoth APT, as it was unclear whether the affected organizations reported the incident to the appropriate authorities. Therefore, this thesis confirms policy timelines for reporting cyber incidents and data breaches are not adequately enforced.

Next, Chapter II states the NPC's Compliance and Monitoring Division evaluates the compliance of the personal information controller when a data breach is reported, and the Complaints and Investigation Division (CID) investigates further if necessary. The NPC issues a decision, order, or resolution for the personal information controller to follow, while the Compliance and Monitoring Division ensures compliance. Based on the findings in Chapter III, the NPC issued a CID order to COMELEC, JFC, and Wendy's, but a CID order for Cebuana Lhuillier was not identified. Since Cebuana Lhuillier's data breach incident was contained, as the main servers were not affected, and transaction details were safe, perhaps it was not necessary for the CID to investigate further. As a result, it is worth noting that COMELEC, JFC, Wendy's, and Cebuana Lhuillier did report their respective cyber incident to the appropriate authorities, the Philippine government responded and provided guidance to help resolve the situation, and in each case, the problem was resolved. Thus, in some respect, cybersecurity and data privacy policies are being enforced and benefitting the Philippines.

Chapter II mentions the CICC facilitates international cooperation in intelligence, investigations, and capacity building. Its Investigation Division serves as the lead unit in cybercrime investigations, assisting law enforcement agencies in special cybercrime cases. Based on the research in Chapter III, the CICC was only mentioned in the COMELEC case where the offenders were identified. It is unknown if CICC was involved in the JFC,

Wendy's, Cebuana Lhuillier, and LuminousMoth APT data breaches. Perhaps those four cases were not considered special cybercrime cases, explaining why the CICC was not mentioned. Nonetheless, in the Wendy's, Cebuana Lhuillier, and LuminousMoth APT data breaches, the Philippine government lacked the ability to identify offenders and hold them accountable for their actions. These results are like the issues addressed in the literature review, which states there is a lack of capacity to pinpoint the main actors conducting cyberattacks against the Philippines. On the contrary, this thesis does confirm domestic actors were responsible for the COMELEC and JFC data breaches, while a Chinese-speaking actor was linked to the LuminousMoth APT.

B. POLICY

Chapters II and III highlighted issues with the reporting and collecting of incident reports and data breach reports. Thus, there may be room for improvement regarding timeliness in incident and data breach reporting, the processing time for the NPC's decisions, orders, or resolutions, and conducting investigations. Further, the responses of government agencies were reactive rather than proactive in dealing with cybersecurity issues. This was noticed when the Philippine government relied on targeted organizations to report cyber incidents, resulting in delays. The Philippine government has policies and procedures to help resolve cyberattacks after a breach has occurred. However, the policies lacked adequate security measures, such as continuous monitoring and enforcement mechanisms, to prevent cyberattacks from occurring. Implementing more robust security measures and regularly testing systems for vulnerabilities may benefit private and public organizations, including the Philippine government.

Other proactive opportunities for improvement include the Philippine government focusing and investing in appropriate protection mechanisms, particularly in digital services and essential services. For the protection of digital services and essential services, the Philippine government may benefit from having the power to supervise public and private digital service providers and operators of essential services to ensure they are implementing cyber security requirements. The Philippine government may benefit from legislation that mandates digital service providers and operators of essential services to

deliver regular evidence of the effective implementation of cyber securities, such as audit results, documentation, and specific reports. A legal act that warrants digital service providers and operators of essential services responsible for managing cyber risks and implementing cyber security requirements may also help improve protection mechanisms. Like any other country, the Philippines continues to face cybersecurity challenges that require policies to be consistently assessed and updated to keep up with evolving cyber threats.

Although the DICT provides external groups information, brochures, and materials about the CERT's purpose and services offered, that does not mean stakeholders are fully aware of the reporting requirements. Therefore, drills or live training in reporting cyber incidents and data breaches may help improve timeliness and real-time reporting. Following from that, perhaps increasing the government's cybersecurity capacity and budget may be worthwhile, since the Philippines faces several challenges, such as low prioritization of cybersecurity concerns, digital transformation surpassing cybersecurity innovation, stagnant budgets for cybersecurity despite rising cyber risks, compatibility issues with legacy systems, and reluctance to experiment with untested solutions.[204] To prevent future breaches, potential methods include giving greater priority to cybersecurity concerns, collaborating with the Forum of Incident Response and Security Teams or Asia Pacific CERT organizations, upgrading cybersecurity systems, enhancing talent and practical skills, and increasing awareness and education about data privacy and cybersecurity risks among organizations and the public.

Next, collaboration and information-sharing between organizations and government agencies ought to be improved to detect and respond to cyberattacks more effectively. The Philippine government has difficulties tracking down the source of cyberattacks, and its ability to identify and hold offenders accountable for cyberattacks needs improvement. This is an issue that the Philippine government may want to address. The involvement of CICC in the JFC, Wendy's, Cebuana Lhuillier, and LuminousMoth

[204] Castillo, "Philippine Cybersecurity in Retrospect (2016-2021)."; Cisco 2018 Asia Pacific Security Capabilities Benchmark Study, 33.

APT data breaches remains uncertain. If CICC was not involved, their participation might have aided in identifying the perpetrators for the Wendy's, Cebuana Lhuillier, and LuminousMoth APT data breaches. On the other hand, if they were involved but unable to identify the perpetrators, there may be opportunities to enhance procedures and resources for detecting cybercriminals. Generally, cybercriminals are less likely to attack when there are high chances of getting caught and severe consequences.

C. RESEARCH LIMITATIONS AND AREAS FOR FURTHER RESEARCH

This thesis was limited to unclassified, open-sourced material. Exploring classified, sensitive, or confidential material regarding this study may provide valuable insight into the Philippine government's effectiveness in addressing cyber threats. During the research process, limited information was readily available to examine the five significant cyberattacks, making it difficult to determine the full extent of how effective the Philippine government and affected organizations were in confronting the cyberattacks. Classified, sensitive, or confidential information may show evidence of which aspects of cyber-related policies were practical or inadequate and where gaps occurred.

Analyzing other cyberattacks or case studies regarding the Philippines' cybersecurity performance may also provide new insight into the Philippine government's effectiveness. Comparing different countries to one another on their effectiveness in addressing cyber threats may lay out best practices and trends for concerns, allowing governments to learn from one another to make better-informed decisions and policies in their cybersecurity practices. Studies on other countries may help shape legislation, policies, agencies, and processes regarding cybersecurity and cyber threats.

This thesis only focused on the government's cybersecurity capabilities in the Philippines and did not explore the cybersecurity of private companies and individuals. There are opportunities to research the effectiveness of the collaboration between the government, private companies, and other stakeholders in addressing cyber threats or cybersecurity challenges. Further research may also include the behavior of individuals and their preparedness in responding to cyber threats.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abuda, Ben Fermin Q., Kareen D. Rivera, and Roselle V. Noroña. "Predictive Validity of a Cybercrime Awareness Tool: The Case of Senior High School Students in a Philippine Secondary School," *International Journal in Information Technology in Governance, Education and Business* 2, no. 1 (January 2020): 18–26, https://ssrn.com/abstract=4007646.

_____. "Advanced Persistent Threat Group LuminousMoth Targeting Government Organization from the Philippines." GOVPH. Last modified July 15, 2021. https://www.ncert.gov.ph/2021/07/15/advanced-persistent-threat-group-luminousmoth-targeting-government-organizations-from-the-philippines/.

Averia, Angel S., Gamaliel Pascual, William Emmanuel Yu, Mary Grace Mirandilla-Santos, Angelo Niño Gutierrez, Bas Claudio, Dan Mejes, and Froland Tajale. *Cybersecurity in the Philippines: Global Context and Local Challenges*. San Francisco, CA: The Asia Foundation, 2022. https://asiafoundation.org/publication/cybersecurity-in-the-philippines-global-context-and-local-challenges/.

Bocar, Vida Zora G. "Breach Management and Reporting." National Privacy Commission. Accessed September 19, 2022. https://www.privacy.gov.ph/wp-content/files/attachments/ppt/DPO5-BreachManagement.pdf.

Cahiles-Magkilat, Bernie. "NPC to Render Decision on Facebook Data Breach." Manila Bulletin. Last modified August 18, 2018. https://mb.com.ph/2018/08/18/npc-to-render-decision-on-facebook-data-breach/.

Camarines, Teressa and John Camarines. "Discussing data Security and Telehealth during the COVID-19 Pandemic." *Journal of Public Health*, (July 2021): 1–2, https//doi.org/10.1093/pubmed/fdab284.

Castillo, Christine. "Philippine Cybersecurity in Retrospect (2016-2021)." GOVPH. Last accessed February 28, 2023. https://www.ndcp.edu.ph/philippine-cybersecurity-in-retrospect-2016-2021/#:~:text=In%20relation%2C%20a%202021%20study,capacity%20to%20manage%20cyber%20threats.

_____. Cebuana Lhuillier Confirmed Hacked in Their Database." Litrato Philippines. Last modified January 19, 2019. https://litratopilipinas.wordpress.com/2019/01/19/cebuana-lhuillier-confirmed-hacked-of-their-database/.

CICC Cybercrime Investigation and Coordinating Center. *Citizen's Charter*. 1st ed. Manila, Philippines: Cybercrime Investigation and Coordinating Center, 2021. https://cicc.gov.ph/wp-content/uploads/2022/11/Final_CICC_Citizens-Charter_2021_June-29-July-2-11_03-AM.pdf.

_____. *Cisco 2018 Asia Pacific Security Capabilities Benchmark Study: Regional Breach Readiness*. San Jose, CA: CISCO, 2018. https://www.cisco.com/c/dam/global/en_au/products/pdfs/cisco_2018_asia_pacific_security_capabilities_benchmark_study.pdf.

CNN Philippines Staff. "Wendy's PH Website Hack Exposes Thousands of Personal Data." CNN. Last modified May 9, 2018. https://www.cnnphilippines.com/business/2018/05/08/wendys-jollibee-website-hack-delivery.html.

_____. "Comelec Data Leaked by Hackers," Rappler, last modified March 28, 2016, https://www.rappler.com/nation/elections/127315-comelec-data-hackers/.

Cruz, RG. "Comelec to Report Data Leaks to Privacy Body." ABS-CBN News. Last modified April 26, 2016. https://news.abs-cbn.com/halalan2016/nation/04/26/16/comelec-to-report-data-leaks-to-privacy-body.

Cybercrime Investigation and Coordinating Center. "About Us Organizational Chart." Accessed December 24, 2022. https://cicc.gov.ph/organizational-chart/.

Department of Information and Communications Technology. *Citizen's Charter*. 1st ed. Quezon City, Philippines: Department of Information and Communications Technology, 2022. https://dict.gov.ph/wp-content/uploads/2022/04/DICT-Citizen_s-Charter.pdf.

———. *DICT Computer Emergency Response Team (CERT) Manual*. Quezon City, Philippines: Department of Information and Communications Technology, 2017. https://www.ncert.gov.ph/cert-manual/dictcertmanual.pdf.

———. *Information Booklet*. Quezon City, Philippines: Department of Information and Communications Technology, 2018. https://dict.gov.ph/wp-content/uploads/2018/03/What-is-DICT.pdf.

Department of Information and Communications Technology National Computer Emergency Response Team. *CERT-PH Incident Reporting and Technical Assistance Request Guidelines*. Version 1.0. Quezon City, Philippines: Department of Information and Communications Technology, 2020. https://www.ncert.gov.ph/wp-content/uploads/2020/06/CERT-PH-Incident-Reporting-and-Technical-Assistance-Request-Guidelines.pdf.

Diop, Serigne, Jema Ndibwile, Doudou Fall, Shigeru Kashihara, and Youki Kadobayashi. "To Coerce or Not to Coerce? A Quantitative Investigation on Cybersecurity and Cybercrime Legislations Towards Large-Scale Vulnerability Notifications." *IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, (October 2019): 282–287. https//doi.org/10.1109/ISSREW.2019.00085.

Domingo, Francis. “Strategic Considerations for Philippine Cyber Security.” *ADRInstitute for Strategic and International Studies* 9, no. 1 (January 2016): 1–14. https//doi.org/10.13140/RG.2.1.4636.7768.

Domingo, Katrina. “Cebuana Lhuillier Bares Data Breach, Tells Clients to Secure Accounts.” ABS-CBN News. Last modified January 19, 2019. https://news.abs-cbn.com/business/01/19/19/cebuana-lhuillier-bares-data-breach-tells-clients-to-secure-accounts.

_____. E-Governance Academy Foundation Company. “National Cyber Security Index.” Accessed March 11, 2023. https://ncsi.ega.ee/country/ph/.

Fabe, Amparo and Ella Zarcilla-Genecela. “The Philippines’ Cybersecurity Strategy.” In *Routledge Companion to Global Cyber-Security Strategy*, edited by Scott N. Romaniuk and Mary Manjikian, 315–324. New York: Routledge, 2021.

Gonzales, Gelo. “Jollibee Deliver website Suspended Over ‘Serious Vulnerabilities.’” Rappler. Last modified May 8, 2018. https://www.rappler.com/technology/202061-national-privacy-commission-jollibee-delivery-website-suspension/.

GOVPH. “Cybercrime Investigation and Coordinating Center (CICC).” Accessed December 24, 2022. https://dict.gov.ph/cybercrime-investigation-and-coordinating-center-cicc/.

———. “Total Number of Incidents from January to December 2021.” Accessed September 18, 2022. https://www.ncert.gov.ph/statistics/.

Haciyakupoglu, Gulizar and Michael Raska. “China’s Political Warfare in Taiwan Strategies, Methods and Global Implications.” In *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, edited by Mikael Weissmann, Niklas Nilsson, Björn Palmerts, and Per Thunholm, 173–194. London: I. B. Tauris, 2021.

Jacob, Jamael and Jessamine Pacis. *Revisiting the Breach: A Briefing Paper on the 2016 COMELEC Data Leak*. Quizon City, PH: Foundation for Media Alternatives, 2017. https://www.fma.ph/wp-content/uploads/2018/04/comeleak-final-1.pdf.

Labong, Ronel. “Identity Theft Protection Strategies: A Literature Review,” *Journal of Academic Research* 4, no. 2 (June 2019): 1–12. https://jar.ssu.edu.ph/index.php/JAR/article/view/1.

Lago, Cristina. “The Biggest Data Breaches in Southeast Asia.” CIO. Last modified January 18, 2020. https://www.cio.com/article/222022/the-biggest-data-breaches-in-the-asean-region.html.

Li, Jia. "Cybercrime in the Philippines: A Case Study of National Security," *Turkish Journal of Computer and Mathematics Education* 12, no. 11 (May 2021): 4224–4231, https://www.turcomat.org/index.php/turkbilmat/article/view/6550/5407.

Lin, Bonny, Christina L. Garafola, Bruce McClintock, Jonah Blank, Jeffrey W. Hornung, Karen Schwindt, Jennifer D.P. Moroney, Paul Orner, Dennis Borrman, Sarah W. Denton, and Jason Chambers. *Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific*. Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/pubs/research_reports/RRA594-1.html.

Lopez, Melissa. "BSP Says Cebuana Lhuillier Data Breach 'Contained.'" BusinessWorld Publishing. Last modified January 28, 2019. https://www.bworldonline.com/banking-finance/2019/01/28/210934/bsp-says-cebuana-lhuillier-data-breach-contained/.

Manantan, Mark B. "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea." *Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs* 56, no. 3 (September 2020): 1–29. https://doi.org/10.1142/S1013251120400135.

Medillo, Luis. "Cebuana Lhuillier Data Breach Affects 900,000 Customers." Tech Pilipinas. Last modified January 19, 2019. https://techpilipinas.com/cebuana-lhuillier-data-breach/.

Misalucha-Willoughby, Charmaine and Francis Domingo. *Enhancing Australia-Philippine Cooperation: Diversifying Strategic Options*. Manila, Philippines: Stratbase ADRi Publications, 2019.

National Privacy Commission. *2021 Rules of Procedures of the National Privacy Commission*. Quezon City, Philippines: National Privacy Commission, 2021. https://www.privacy.gov.ph/wp-content/uploads/2021/01/2021rulesofprocedure_VER8-Final-Sgd-1-1-1.pdf.

———. "About Us National Privacy Commission." Accessed September 6, 2022. https://www.privacy.gov.ph/about-us/#quality_policy.

———. *Citizen's Charter*. 1st ed. Manila, Philippines: National Privacy Commission, 2021. https://www.privacy.gov.ph/wp-content/uploads/2022/05/npc-citizens-charter_1st-Edition.pdf.

———. "Exercising Breach Reporting Procedures." Accessed September 19, 2022. https://www.privacy.gov.ph/exercising-breach-reporting-procedures/.

_____. Official Statement of Privacy Commissioner Raymund Enriquez Liboro on the Cebuana Lhuiller Breach." GovPH. Last modified November 11, 2021. https://www.privacy.gov.ph/2019/01/official-statement-of-privacy-commissioner-raymund-enriquez-liboro-on-the-cebuana-lhuiller-breach/.

Osborne, Charlie. "Chinese APT LuminousMoth Abuses Zoom Brand to Target Gov't Agencies." ZDNET. Last modified July 16, 2021. https://www.zdnet.com/article/chinese-apt-luminousmoth-abuses-zoom-brand-to-target-govt-agencies/.

Pan, Chongxia, Weijun Zhong, and Shue Mei. "Finding the Weakest Link in the Interdependent Security Chain Using the Analytic Hierarchy Process," *Journal of Advances in Computer Networks* 3, no. 4 (December 2015): 320 – 325. https://doi.org/10.18178/JACN.2015.3.4.190.

Permata, Inda M. and Bima J. Nanda. "The Securitization of Cyber Issue in ASEAN." In *A 2019 Proceeding of the 1st International Conference of ASEAN*, 90–97. Padang, West Sumatra, Indonesia. Warsaw: Sciendo, 2009. https://doi.org.10.1515/9783110678666-012.

_____. "*Philippine Privacy Regulator Suspends Jollibee's Online Delivery Site*." S&P Global. Last modified May 7, 2018. https://www.spglobal.com/marketintelligence/en/news-insights/trending/yjT6xL9pGN5rP4OOIlgaBA2.

_____. Philippines Crime and Security Risk Report Q1 2020 in Fitch Solutions. FSG 08789939. London, UK: Fitch Solutions, 2019. www.fitchsolutions.com.

_____. Philippines News Agency. "PH 4th Among Countries Most Targeted by Web Threats." February 21, 2022. https://www.pna.gov.ph/articles/1168257.

_____. "Privacy Commission Recommends Criminal Prosecution of Bautista Over "Comeleak"." Gov.PH. Last modified November 11, 2021. https://www.privacy.gov.ph/2017/01/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/.

Punzalan, Jamaine. "NBI Arrests 2nd Hacker in Comelec Data Breach." ABS-CBN News. Last modified April 29, 2016. https://news.abs-cbn.com/halalan2016/nation/04/29/16/nbi-arrests-2nd-hacker-in-comelec-data-breach.

Obet, Dedy and Henri Mujoko Suharto. "Cyber Cooperation in the Framework of the ASEAN Regime," *Jurnal Pertahanan* 7, no. 2 (August 2021): 254–261, http://dx.doi.org/10.33172/jp.v7i2.1264.

Omorog, Challiz, Camarines Sur, and Ruji Medina. "Internet Security Awareness of Filipinos: A Survey Paper," *International Journal of Computing Science Research* 1, no. 4 (March 2018): 14–26, https://doi.org/10.25147/ijcsr.2017.001.1.18.

Ramadhan, Iqbal. "Building Cybersecurity Regulations in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)," *Journal of Social and Political Sciences* 3, no. 4 (December 2020): 983–995, https://doi.org/10.31014/aior.1991.03.04.230.

_____. "Rare, Mass Advanced Threat Campaign Targets More Than a Thousand Users in Southeast Asia," Kaspersky, July 14, 2021, https://www.kaspersky.com/about/press-releases/2021_rare-mass-advanced-threat-campaign-targets-more-than-a-thousand-users-in-southeast-asia.

Salsabila, Anna S., Muflih D. Fikri, Muhammad S. Andika, and Nanda A. Harahap. "Potential and Threat Analysis Towards Cybersecurity in South East Asia," *Journal of ASEAN Dynamics and Beyond* 1, no. 1 (June 2020): 1–12, https://doi.org/10.20961/aseandynamics.v1i1.46794.

Serzo, Aiken. "Philippine Regulations for Cross-border Digital Platforms: Impact and Reform Considerations." *Philippine Institute for Development Studies* 1, no. 1 (October 2021): V-41, https://www.pids.gov.ph/publication/research-paper-series/philippine-regulations-for-cross-border-digital-platforms-impact-and-reform-considerations.

_____. "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, 2022, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Singh, Meelendra. Understanding Data Privacy to Advance Customer Protection in Vietnam, Indonesia and the Philippines. Bonn and Eschborn, Germany: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, 2020. https://www.mefin.org/docs/data-privacy-report-vip.pdf.

Smith, Robert, Mark Perry, and Nucharee Smith. "Three Shades of Data: Australia, Philippines, Thailand," *Singapore Journal of Legal Studies* 1, no. 1 (March 2021): 76–99. https://www.proquest.com/scholarly-journals/three-shades-data-australia-philippines-thailand/docview/2529334510/se-2?accountid=12702.

Thinyane, Mamello and Debora Christine. *Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies*. Macau: United Nations University, 2020. http://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf.

Vaas, Lisa. "Fake Zoom App Dropped by New APT 'LuminousMoth.'" Threatpost. Last modified July 15, 2021. https://threatpost.com/zoom-apt-luminous-moth/167822/.

_____. "Wendy's PH Informs Users of Site Data Breach after NPC Intervention." Rappler. Last modified May 8, 2018. https://www.rappler.com/technology/202040-wendys-philippines-data-breach/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California