GET INTERNATIONAL RESEARCH JOURNAL

RESPONSIVENESS OF CYBER SECURITY OPERATION CENTER OF THE PHILIPPINE NATIONAL POLICE TO DATA BREACHES: BASIS FOR ENHANCEMENT

Michelle Bensay Sanico[1]
[1]Philippine College of Criminology, #641 Sales Street, Sta. Cruz, Manila, Philippines

Corresponding Email: bensaymichelle@gmail.com

Available Online: November 2025
Revised: October 2025
Accepted: October 2025
Received: September 2025

Volume III Issue 4 (2025)
DOI: 10.5281/zenodo.17914026
E-ISSN: 2984-7184
P-ISSN: 2984-7176
GET International Research Archives

Abstract

The study titled "Responsiveness of the Cyber Security Operation Center of the Philippine National Police to Data Breaches: Basis for Enhancement" evaluated how effectively the PNP CSOC addresses data breaches, the challenges it faces, and areas for improvement. Using a descriptive qualitative approach, the researchers gathered data from 45 PNP personnel through surveys and interviewed 5 CSOC staff. The investigation covered four major domains: Detection and Analysis; Mitigation, Isolation, and Recovery; Post-Incident Activity; and Prevention and Monitoring. Results showed that while real-time monitoring and machine-learning tools supported effective detection, issues such as high data volume, alert fatigue, complex threats, limited system visibility, and inadequate training remained. Mitigation and recovery protocols worked well for familiar threats but were less effective for emerging attacks, with delays in restoring systems and insufficient automation. Post-incident procedures lacked consistency due to missing standardized templates and limited time, though sharing insights and lessons learned was practiced. Prevention and monitoring strategies functioned adequately but required more advanced detection tools, regular updates, and stronger threat intelligence integration. Overall, the study found that although the PNP CSOC has a solid foundation, improvements in technology, training, policy development, procedures, and inter-agency cooperation are essential. Recommendations focused on upgrading cybersecurity tools, enhancing continuous training, formalizing protocols, strengthening threat intelligence sharing, and increasing resources.

Keywords: *Cyber Security Operation Center (CSOC), Data Breaches, Incident Response*

Recommended Citation:
Sanico, M. B. (2025). RESPONSIVENESS OF CYBER SECURITY OPERATION CENTER OF THE PHILIPPINE NATIONAL POLICE TO DATA BREACHES: BASIS FOR ENHANCEMENT. GET INTERNATIONAL RESEARCH JOURNAL, 3(4), 189–202. https://doi.org/10.5281/zenodo.17914026

INTRODUCTION

The philosophical foundation of this study rests on Pragmatism, which emphasizes the practical application of knowledge to resolve real-world problems (Creswell, 2013), and Critical Realism, which acknowledges that while cyber threats are socially constructed in their perception, they are grounded in objective realities that demand systematic response (Clandinin & Connelly, 2000). Guided by these perspectives, the research views the Cyber Security Operation Center (CSOC) not merely as a technical apparatus but as a socio-technical part of the PNP Organization whose effectiveness must be measured by its capacity to safeguard public trust, uphold legal mandates such as the Data Privacy Act of 2012, and ensure national resilience against evolving cyber threats (Sy, 2020; PCIJ, 2021). By situating the evaluation within the incident response lifecycle outlined by the NIST Computer Security Incident Handling Guide (SP 800-61) (NIST,2012) and the ISO/IEC 27035 Incident Management Framework (ISO, 2023), the study underscores the philosophical imperative that knowledge and policy must converge to produce actionable strategies. In this way, theory informs practice, and practice validates theory, ultimately advancing both criminological scholarship and institutional cybersecurity governance (ENISA, 2020; SANS, 2021).

In the contemporary era, the pervasive and accelerating adoption of digital technologies globally has dramatically escalated the incidence and sophistication of cyberattacks, presenting profound security challenges for nations worldwide (DOST, 2023; UNDP, 2022). As a dynamic and rapidly developing economy, the Republic of the Philippines is highly integrated into the global digital ecosystem, consequently facing heightened susceptibility to a diverse array of cyber threats, from petty cybercrime to advanced persistent threats targeting critical governmental systems. These threats not only cause significant financial losses but also pose a serious risk to national security and undermine public trust (NPC, 2022; PCIJ, 2021; Sy, 2020). The evolving nature of cybercriminal tactics necessitates continuous and urgent enhancement of national cybersecurity capabilities and effective Incident Response mechanisms.

Acknowledging this critical need, the Philippine National Police (PNP) established the provisional Cyber Security Operation Center (CSOC) in 2024 as part of its ICT Master Plan Information System Strategic Plan for 2023–2025 (PNP, 2023). The CSOC functions as a centralized hub for real-time monitoring, proactive detection, and coordinated response to cyber incidents affecting government networks and critical information infrastructure. Between June and December 2024 alone, the CSOC detected and addressed 4,625 cybersecurity threats, underscoring both the scale of the challenge and the critical importance of its mission (PNP, 2023).

The CSOC's pivotal role involves maintaining situational awareness, sharing threat intelligence, and coordinating incident handling across various government entities to ensure the resilience of the nation's digital assets.

However, the effectiveness and efficiency of the CSOC's capabilities, particularly concerning Data Breaches, one of the most prevalent and impactful types of cyber incidents, remains a crucial area for evaluation. Data breaches involve the unauthorized access or disclosure of sensitive information, with repercussions extending far beyond immediate financial costs to include severe reputational damage, regulatory penalties under the Philippine Data Privacy Act of 2012 (NPC, 2022), and operational disruption.

Therefore, this research was designed to conduct a comprehensive assessment of the responsiveness and overall effectiveness of the PNP's provisional CSOC specifically in the context of data breach incidents. Guided by internationally recognized frameworks such as National Institute of Standards and Technology (NIST) SP 800-61 and ISO/IEC 27035 (NIST, 2012; ISO, 2023), the evaluation was multi-faceted examining performance across key phases

of the incident response lifecycle drawn from the NIST framework. The primary areas of evaluation encompassed the CSOC's capabilities in Detection and Analysis; Mitigation, Isolation, and Recovery; Post-Incident Activity; and Preparation and Monitoring. The ultimate goal of this research was to identify systemic and operational gaps, benchmark current practices against national and international standards, and provide specific, actionable recommendations to strengthen the PNP's cybersecurity posture and ensure greater digital resilience throughout the Philippines (ENISA, 2020; SANS, 2021).

Objectives

This study was conducted to evaluate the responsiveness and effectiveness of the Philippine National Police (PNP) provisional Cyber Security Operations Center (CSOC) in addressing data breaches, with the ultimate goal of identifying areas for enhancement.

Specifically, this study aimed to answer the following questions:

1. Detection and Analysis – How effective is the CSOC in detecting and analyzing data breaches, including its ability to identify suspicious activity, assess scope, and interpret threat actor tactics, techniques, and procedures (TTPs)?
2. Mitigation, Isolation, and Recovery – How responsive is the CSOC in containing, isolating, and recovering from data breaches once detected, and what challenges are encountered in these processes?
3. Post-Incident Activity – To what extent does the CSOC conduct thorough post-incident reviews, documentation, and lessons learned to strengthen future preparedness?
4. Prevention and Monitoring – What proactive measures, such as continuous monitoring, vulnerability management, and personnel training, are implemented by the CSOC to prevent future data breaches?
5. Enhancement Basis – What specific technological, organizational, and policy improvements can be recommended to enhance the CSOC's responsiveness and align its practices with international standards and best practices?

METHODS

A qualitative methodology was adopted, utilizing validated survey questionnaires and in-depth interviews. The survey was administered to forty-five (45) personnel from the Cybersecurity Management Division (CMD) and Cyber Security Operation Center (CSOC) of the Directorate for Information and Communications Technology (DICTM), and selected staff from Information Technology Management Service (ITMS), while five (5) highly experienced CSOC staff were interviewed to provide deeper insights. The survey included open-ended questions to capture broader perspectives, while interviews allowed for detailed exploration of individual experiences and operational challenges (Pahi et al., 2017; Hawamleh et al., 2020). Document analysis of official incident response plans and post-incident reports complemented the primary data sources. The research investigated the tools, processes, and methodologies utilized by the CSOC in each of these phases.

This study employed a narrative inquiry research design to explore the experiences of personnel within the Philippine National Police (PNP) Cyber Security Operations Center (CSOC) regarding challenges in detecting, mitigating, and addressing data breaches. Narrative inquiry, as a qualitative approach, emphasizes understanding human experience through the stories individuals tell about their lives (Clandinin & Connelly, 2000; Creswell, 2013). This design was

chosen to capture the nuanced realities of CSOC personnel, focusing on their lived experiences, perceptions, and meaning-making processes in the context of cybersecurity incident response.

POPULATION OF THE STUDY. The population of the study consisted of two groups of PNP personnel involved in CSOC operations and response coordination. The study utilized two primary data gathering tools. A Survey Questionnaire was administered to a broader sample of forty-five (45) respondents, comprising personnel from Cybersecurity Management Division (CMD), analysts of Cyber Security Operations Center (CSOC), selected Information and Technology Project Officers (ITPOs), and selected Information and Technology Management Service (ITMS) personnel, to gather perspectives across the four phases of incident response. Subsequently, In-depth, semi-structured Interviews were conducted with five (5) selected key informants from CSOC to delve into specific experiences and insights regarding challenges, preparedness, and capability. Purposive sampling was employed to select participants based on expertise, experience, and direct involvement in incident response (Purposive Sampling Guide, 2016).

Table 1

Population of the Study

Population	**Size**	**Sampling Technique**
CMD Personnel	7	Survey Questionnaire
CSOC Personnel	17	Survey Questionnaire
Selected ITMS/ITPO Personnel	21	Survey Questionnaire
DICTM Selected Personnel	5	Interview
Total	50	

LOCALE OF THE STUDY. The study was conducted at the PNP Cyber Security Operations Center (CSOC), located on the 2nd Floor of the NHQ Building, DICTM Annex, Camp BGen Rafael T. Crame, Quezon City. This site was selected as it serves as the central hub for monitoring, detecting, and coordinating responses to cyber threats affecting PNP digital assets (PNP, 2023). Its institutional significance and access to operational data made it an ideal setting for evaluating responsiveness and effectiveness.

TREATMENT OF THE DATA. The treatment of the data involved two main approaches. For the quantitative data gathered from the Likert scale items in the survey, descriptive statistical analysis was used. For the qualitative data gathered from the open-ended survey questions and the in-depth interviews (addressing challenges, preparedness, and capability), thematic analysis was employed. This involved systematically reading, analyzing, and reporting patterns (themes) within the data.

The findings from both the quantitative and qualitative analyses were then integrated to provide a comprehensive understanding of the CSOC's effectiveness and to form the basis for the proposed recommendations, directly addressing the "basis for enhancement" aspect of the study.

SCOPE AND LIMITATIONS. The study focused on four operational areas derived from established incident response frameworks: Detection and Analysis; Mitigation, Isolation, and Recovery; Post-Incident Activity; and Prevention and Monitoring (NIST, 2012; ISO, 2023).

Limitations included:

- **Geographical focus** restricted to Camp Crame, limiting generalizability to other agencies.
- **Self-reported data**, which may introduce subjective bias.
- **Dynamic nature of cyber threats**, meaning findings reflect practices at a specific point in time.
- **Access restrictions** to sensitive technical details due to confidentiality.
- **Limited scope of inter-agency collaboration analysis**, focusing primarily on CSOC's internal operations.

DATA GATHERING TOOLS. Two instruments were employed:

1. **Survey Questionnaire** – administered to 45 respondents, combining quantitative ratings with qualitative explanations.
2. **In-depth Interview Guide** – conducted with 5 key informants, audio/video recorded for accuracy.

Both tools were aligned with the study's conceptual framework and research questions (Qualitative Methods Text, 2020; Phenomenology Guide, 2018). Ethical considerations were strictly observed, including informed consent, confidentiality, and Institutional Review Board (IRB) approval (Ethical Research Guide, 2019).

RESULTS and DISCUSSION

Global scholarship consistently emphasizes the escalating complexity of cyber threats in the digital era. Reports from the International Telecommunication Union (ITU, 2023) and the World Economic Forum (WEF, 2024) highlight the increasing frequency and sophistication of cyber incidents, including large-scale data breaches and disruptive attacks across government, finance, healthcare, and critical infrastructure. These incidents inflict substantial economic losses, compromise sensitive information, and erode public trust in institutions.

Studies underscore the dual challenge faced by Security Operations Centers (SOCs): technological sophistication and human resource limitations. ENISA (2020) and SANS (2021) note that SOCs worldwide struggle with information overload, alert fatigue, and workforce shortages. Effective detection requires continuous training and investment in advanced tools such as Security Information and Event Management (SIEM) and Data Loss Prevention (DLP) systems. International best practices emphasize automation and orchestration. The U.S. Department of Homeland Security (DHS, 2022) and Singapore's Cyber Security Agency (CSA Singapore, 2021) stress the importance of SOAR platforms, AI-driven detection, and predictive analytics to accelerate containment and recovery. Similarly, the European Union's Cybersecurity Act (EU, 2019) and Digital Services Act (EU, 2022) highlight the need for structured knowledge management, standardized reporting, and cross-agency collaboration.

At the national level, the Philippines has enacted the Cybercrime Prevention Act of 2012 (RA 10175) and established the Cybercrime Investigation and Coordinating Center (CICC Act, 2012). However, challenges persist in harmonizing multi-agency coordination, resource allocation, and technical expertise (Sy, 2020; NPC, 2022; PCIJ, 2021). Local government units, universities, and small businesses remain particularly vulnerable due to limited resources and cybersecurity awareness (Public Trust Journal; Local Govt Cyber Study).

Empirical studies on SOCs and incident response frameworks affirm that the challenges faced by the PNP CSOC are consistent with global experiences. Research on incident response evaluation (NIST, 2012; ISO, 2023) highlights the importance of structured processes across detection, mitigation, post-incident activity, and prevention.

Detection and Analysis: ENISA (2020) and SANS (2021) emphasize that SOCs worldwide struggle with information overload, alert fatigue, and workforce shortages**.** These challenges mirror the PNP CSOC's experience, where real-time monitoring and machine learning are deployed but undermined by data volume and limited analyst training. Studies also underscore the importance of continuous training and investment in SIEM and DLP tools to sustain detection effectiveness.

Mitigation, Isolation, and Recovery :International best practices (DHS, 2022; CSA Singapore, 2021) stress the role of automation, orchestration (SOAR), and AI-driven detection in accelerating containment and recovery. The PNP CSOC's reliance on manual processes and outdated systems reflects the global gap between established protocols and the demands of novel, sophisticated attacks.

Post-Incident Activity: EU (2019) and WEF (2024) emphasize that effective post-incident reviews require standardized templates, structured knowledge management, and formalized intelligence-sharing protocols. The PNP CSOC's inconsistencies in documentation and limited formalization of external coordination align with these findings, underscoring the need for MOUs and intelligence-sharing protocols.

Prevention and Monitoring: ITU (2023) and the Cybersecurity Workforce Book studies highlight that SOC effectiveness is inseparable from continuous training, certification, and retention strategies. The PNP CSOC's training gaps and limited monitoring scope reflect this global concern reinforcing calls for continuous certification programs, vulnerability scanning, and predictive analytics**.**

Collectively, these studies situate the PNP CSOC's challenges within a broader international context, affirming that investment in technology, structured processes, and human capital are critical for resilience against evolving cyber threats.

This study assessed the responsiveness and effectiveness of the Philippine National Police (PNP) Cyber Security Operations Center (CSOC) in handling data breaches. The findings were structured around four phases of incident response: Detection and Analysis, Mitigation/Isolation/Recovery, Post-Incident Activity, and Prevention/Monitoring. Survey and interview data provide quantitative support for the qualitative findings across the four phases of incident handling and were triangulated with international literature to provide a comprehensive evaluation.

RESPONSIVENESS AND EFFECTIVENESS IN DETECTION AND ANALYSIS. In the area of Detection and Analysis, the current mechanisms, which include tools such as real-time monitoring and machine learning, are generally perceived as effective by many personnel. However, this effectiveness is offset by substantial technical and operational challenges, including the overwhelming volume of data, the resultant issue of alert fatigue, the increasing complexity of modern attacks, and a lack of complete network visibility. Furthermore, a critical operational gap identified was the insufficiency and lack of continuous, practical training for CSOC personnel, which is vital for maintaining proficiency against evolving cyber threats.

Survey results revealed that majority of respondents perceived CSOC's detection mechanisms as effective, citing real-time monitoring, automated alerts, and machine learning algorithms. However, some respondents rated detection as only "neutral" or "insufficient," pointing to challenges such as: Data overload and difficulty distinguishing legitimate from malicious activity; Alert fatigue due to numerous false positives; Technical limitations, including reliance on free or unlicensed tools and unstable internet connections; and Human resource gaps, with limited training and

expertise among analysts. Effectiveness ratings skewed positive but with a significant minority expressing dissatisfaction**,** indicating uneven confidence in detection capabilities.

Figure 3.1.A

Effectiveness of the current detection mechanism to identify potential data breaches.

Result:

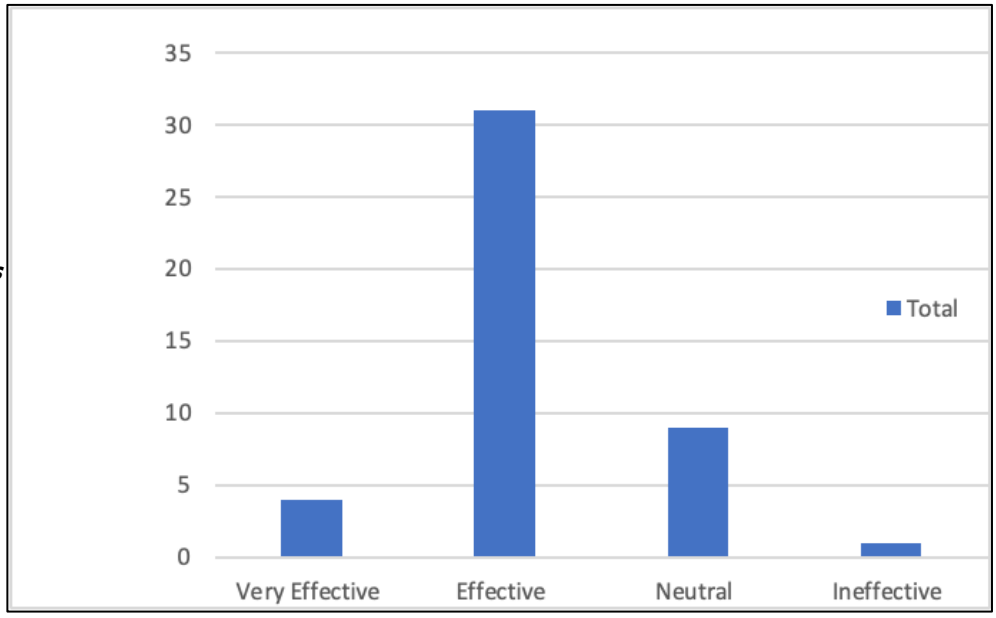

Figure 3.1.A. Effectiveness of the current detection mechanism to identify potential data breaches.

These findings resonate with ENISA (2020) and SANS (2021), which emphasize that SOCs globally struggle with information overload and workforce shortages. The absence of continuous training and advanced tools such as SIEM and DLP was identified as a critical gap. Interviews further highlighted the lack of a fully dedicated incident response team and recommended elevating CSOC's organizational status within the PNP command structure to ensure adequate resources and authority.

MITIGATION, ISOLATION, AND RECOVERY. For Mitigation, Isolation, and Recovery, the study indicated varying levels of protocol effectiveness. The CSOC demonstrated strengths in responding to known or common threats, suggesting adherence to established, basic incident response procedures. Conversely, significant weaknesses were observed in handling novel or sophisticated attacks. Key inhibitors to swift and efficient recovery included noticeable delays in system restoration and a discernible lack of automation in critical response processes.

CSOC's containment protocols were generally rated by respondents as effective to very effective, supported by escalation steps, skilled personnel, and real-time alerts. However, following challenges were identified: Technical limitations: outdated systems, lack of automation, and absence of network log monitoring; Human factors: insufficient skilled professionals, stress in decision-making, and reliance on manual processes; Coordination gaps: slow communication between units and delays in containment; and Resource constraints: limited budget and outdated

hardware/software. Containment scored higher than recovery, suggesting stronger initial response but weaker restoration capacity.

Figure 3.2.A

Effectiveness of PNP CSOC Protocols for Containing Data Breaches

Results:

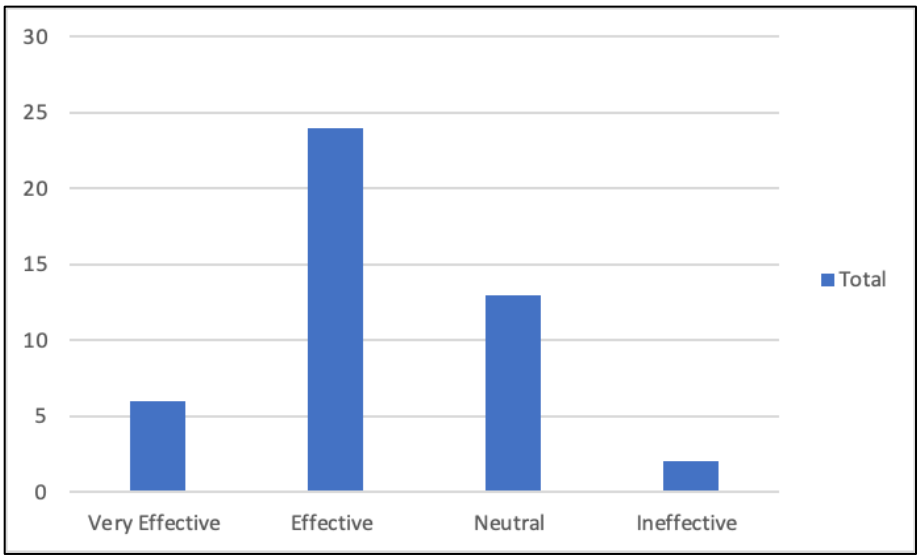

Figure 3.2.A Effectiveness of PNP CSOC Protocols for Containing Data Breaches

Figure 3.2.B

The Overall Recovery Process After a Data Breach Incident of PNP CSOC.

Results:

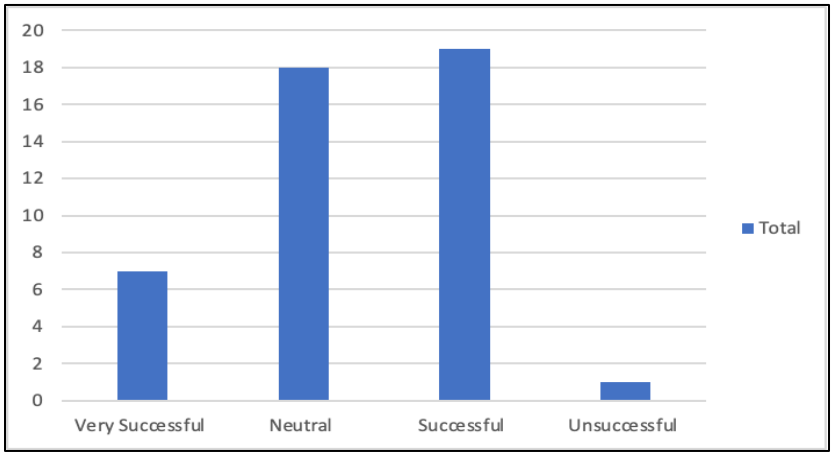

Figure 3.2.B. The Overall Recovery Process After a Data Breach Incident of PNP CSOC.

International best practices emphasize the importance of automation, orchestration (SOAR), and AI-driven detection to accelerate containment and recovery (DHS, 2022; CSA Singapore, 2021). In line with these standards,

respondents underscored the need for advanced technologies such as SOAR and XDR, alongside refined SOPs and regular simulation exercises. These recommendations reflect global incident response practices, where automation and continuous drills are critical to strengthening resilience (DHS, 2022; CSA Singapore, 2021).

POST-INCIDENT ACTIVITY. The Post-Incident Activity phase showed inconsistencies in the thoroughness of reviews conducted after a breach. Challenges here included the absence of standardized templates for documentation and systematic review, as well as time constraints placed on personnel. Despite these inconsistencies, the aspect of sharing "lessons learned" within the organization was generally viewed positively, indicating a culture of improvement, albeit one that lacks formalized structure.

Perceptions of CSOC's post-incident review process varied widely. Some respondents rated reviews as thorough, citing detailed timelines, root cause analysis, and multi-level evaluations. Others noted gaps, including: Lack of standardized templates for reporting; Insufficient time for in-depth reviews.**;** Difficulty translating technical findings for non-technical stakeholders; and Delays in implementing lessons learned.

Coordination with external agencies such as DICT and international partners was acknowledged but described as needing formalization through Memoranda of Understanding (MOUs) and standardized intelligence-sharing protocols. These findings echo EU (2019) and WEF (2024), which stress the importance of structured knowledge management and cross-agency collaboration in effective post-incident activity (EU, 2019; WEF, 2024).

Figure 3.3.A

Post-Incident Review Process Conducted by PNP CSOC

Results:

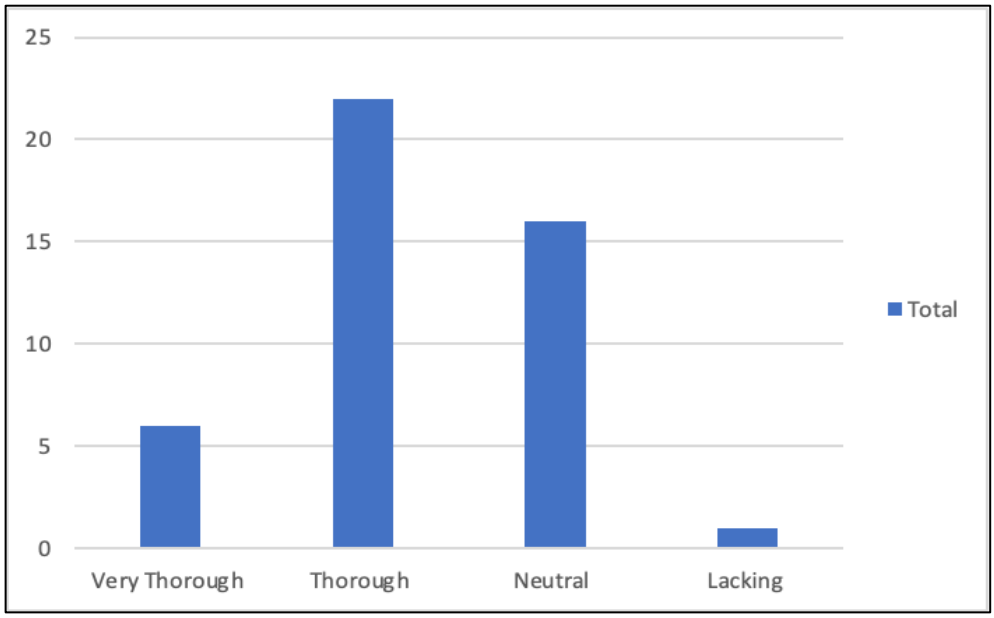

Figure 3.3.A. Post-Incident Review Process Conducted by PNP CSOC

PREVENTION AND MONITORING. Finally, regarding Prevention and Monitoring measures, current practices were deemed effective to an extent, but the findings underscored a strong need for more advanced and

proactive capabilities. Specific needs identified included integrating better threat intelligence to anticipate attacks, implementing more frequent updates of defensive systems, and acquiring enhanced, cutting-edge detection tools to keep pace with the adversary. Interviewed personnel specifically emphasized the necessity for comprehensive capability and capacity enhancement alongside the strategic integration of threat intelligence as core areas for improvement. Collectively, the findings across all four phases demonstrate that operational and procedural enhancements, underpinned by investment in technology and human capital, are crucial to allow the CSOC to effectively fulfill its mandate in the face of persistent and escalating cyber threats.

Respondents emphasized the importance of proactive measures, including continuous vulnerability scanning, penetration testing, and predictive analytics. However, CSOC's current monitoring scope is limited to PNP assets with installed security agents, leaving gaps in coverage.

Training was repeatedly identified as insufficient, with most respondents rating it "neutral" or "insufficient." Calls for continuous training, certification programs, practical exercises, and integration of predictive analytics were strong. These findings reflect global concerns that SOC effectiveness is closely tied to workforce development and retention (Cybersecurity Workforce Book; ITU, 2023).

Figure 3.4.A

Effectiveness of Preventive Measures Currently in place to avoid Data Breach

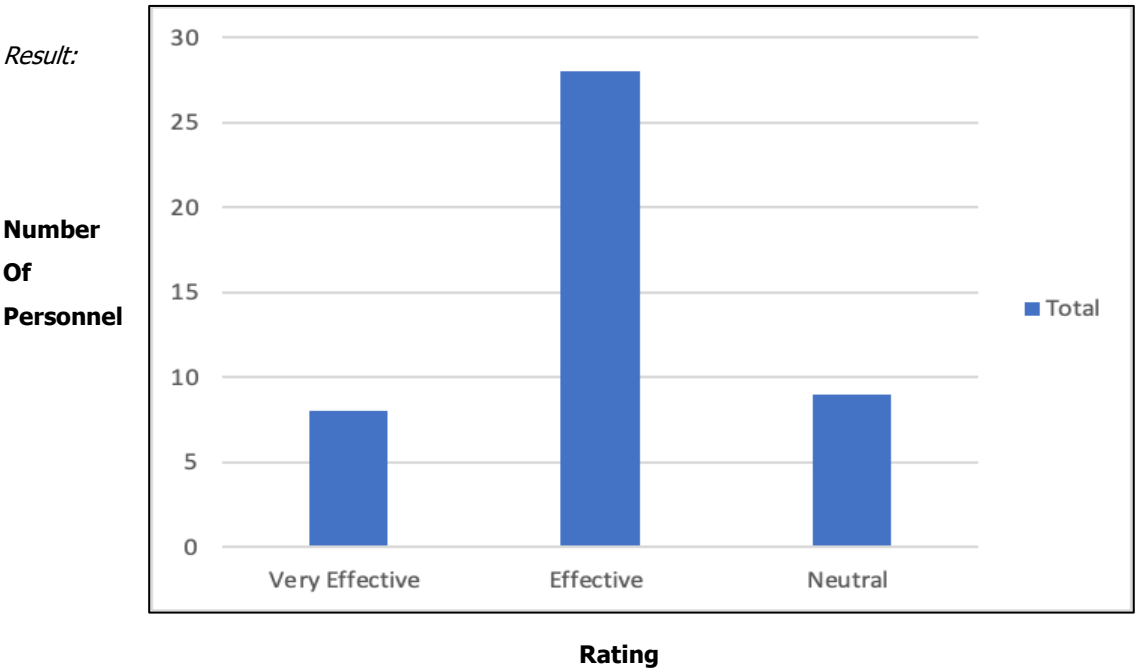

Figure 3.4.A. Effectiveness of Preventive Measures Currently in place to avoid Data Breach

Based on survey and interview data, the findings confirm that while the PNP CSOC has established a foundational structure for incident response, its responsiveness remains constrained by systemic gaps in technology, training, and coordination. Detection and containment are relatively strong, but recovery, post-incident review, and training lag behind. Key recommendations for strengthening CSOC and to addressing these gaps requires the following:

- **Technology enhancement**: Invest in SIEM, DLP, IDS/IPS, UEBA, and cloud security tools.

- **Personnel training or Human capital investment**: Implement continuous, practical training and certification programs.
- **Policy improvement**: Update SOPs, align with international standards, and formalize incident response plans.
- **Coordination**: Strengthen partnerships with national and international agencies; streamline internal reporting.
- **Organizational support**: Elevate CSOC's strategic role within PNP for resource prioritization.
- **Proactive measures**: Conduct regular vulnerability scans, penetration tests, and simulation exercises.

By aligning with international best practices and addressing statistically validated weaknesses, the CSOC can evolve into a more resilient and proactive cybersecurity defense unit capable of safeguarding national digital assets and reinforcing public trust.

CONCLUSION

The study concludes that the PNP Cyber Security Operation Center (CSOC) possesses a fundamental structure for cybersecurity defense but requires substantial strategic enhancements to become fully responsive and effective against the rapidly evolving cyber threat landscape. The current operational environment is challenged by technical limitations (e.g., alert fatigue, lack of visibility), human capital deficiencies (e.g., insufficient training), and procedural inconsistencies (e.g., non-standardized post-incident review). Addressing these gaps is paramount to strengthening the nation's cyber resilience.

It is revealed that while CSOC has established foundational protocols for detection, mitigation, recovery, and post-incident activity, its current capacity remains constrained by technological limitations, resource shortages, and insufficient training. Detection mechanisms were perceived as moderately effective, supported by real-time monitoring and automated alerts, but hindered by alert fatigue, data overload, and reliance on limited tools. Mitigation and recovery protocols were rated as effective by many respondents, yet challenges persisted in automation, coordination, and resource allocation. Post-incident activities demonstrated varying levels of thoroughness, with some structured reviews conducted but lacking standardized templates and consistent dissemination of lessons learned. Preventive measures, including vulnerability scanning and monitoring, were in place but limited in scope, with training repeatedly identified as insufficient. These underscore the infancy stage of CSOC's development and highlight the urgent need for enhancement across five critical areas. The following key recommendations are proposed for the enhancement of the PNP CSOC:

- **Investment in Advances Cybersecurity Tools:** The CSOC must secure greater resource allocation to invest in advanced cybersecurity tools, specifically those that offer superior detection capabilities, threat intelligence integration, and automation of response processes to mitigate alert fatigue and system restoration delays.
- **Continuous and Practical Training Program:** A formalized program for continuous and practical training should be implemented for all CSOC personnel to address the identified gap in capabilities. This training should focus on handling sophisticated, novel attacks and leveraging new technologies.

- **Formalization and Regular Updating of Protocols:** Standard operating procedures for all phases of incident response, especially for post-incident reviews, must be formalized, regularly updated, and enforced to ensure consistency, thoroughness, and effective learning from past incidents.
- **Strengthening Inter-Agency Collaboration:** Efforts must be intensified to strengthen internal (e.g., with PNP Anti-Cybercrime Group) and external collaboration mechanisms to facilitate timely and effective threat intelligence sharing and coordinated incident response with other national and international stakeholders.

By benchmarking against global best practices (NIST, 2012; ISO, 2023; ENISA, 2020; SANS, 2021), the study affirms that enhancing CSOC's responsiveness is not only vital for immediate incident handling but also for fortifying the Philippine National Polices' overall cybersecurity posture. The recommendations derived from this research provide actionable pathways for policy decisions, resource allocation, training initiatives, and operational improvements for PNP provisional CSOC and within the organization.

Ultimately, the responsiveness of the PNP CSOC to data breaches is a cornerstone of national digital resilience. Strengthening its capabilities will safeguard citizen data, protect critical government systems, and reinforce public trust in law enforcement's ability to secure the digital environment. This dissertation contributes to the broader discourse on cybersecurity in developing nations, offering evidence-based insights that can guide the Philippine National Police toward a more robust, adaptive, and internationally aligned cybersecurity framework.

REFERENCES

Alqudhaibi A., Deshpande S., Jagtap S., & Salonitis K. (2023). Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technological Sustainability, 2(4), 372–387. https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/1

Backman, S. B. (2015). Organising National Cybersecurity Centres. Information & Security: An International Journal, 32, 3206-1 to 3206-18. http://dx.doi.org/10.11610/isij.3206

Booc, N.B.B. (2024). Cybersecurity Awareness, and Cybersecurity Behavior of High School Students in Davao City: A Mediation Role of Perceived Behavioral Control. European Journal of Applied Science, Engineering and Technology, 2(3), 4–9.

Clandinin, D. J., & Connelly, F. M. (2000). *Narrative inquiry: Experience and story in qualitative research*. San Francisco, CA: Jossey-Bass.

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Department of Homeland Security (DHS). (2022). *Federal Cybersecurity Operations Center Framework*. Washington, DC: U.S. Government Printing Office.

Department of Science and Technology (DOST). (2023). *Philippine Science and Technology Cybersecurity Report*. Quezon City: DOST.

European Union. (2019). *Cybersecurity Act*. Brussels: EU Publications.

European Union. (2022). *Digital Services Act*. Brussels: EU Publications.

European Union Agency for Cybersecurity (ENISA). (2020). *Incident response best practices*. Athens: ENISA

Publications.

Ethical Research Guide. (2019). *Guidelines for research involving human participants*. [Publisher details].

Godoy, C.H., Lerit, J.C., Jehru, N., Diego, R., & Costales, J.A. (2022, July). Cybersecurity Scientometric Analysis: Mapping of Scientific Articles using Scopus API for Data Mining and Webscrapping. 2022 5th International Conference on Data Science and Information Technology (DSIT 2022). China.

Hawamleh, H., Alqudhaibi, A., & Saeed, M. (2020). Qualitative approaches in cybersecurity research. *Journal of Information Security Studies, 15*(2), 45–60.

International Conference on Industrial Engineering and Operations Management. Singapore, Singapore. https://index.ieomsociety.org/index.cfm/article/view/ID/1122

International Organization for Standardization (ISO). (2023). *ISO/IEC 27035: Information security incident management*. Geneva: ISO.

International Telecommunication Union (ITU). (2023). *Global Cybersecurity Index 2023*. Geneva: ITU.

National Institute of Standards and Technology (NIST). (2012). *Computer Security Incident Handling Guide (SP 800-61)*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology (NIST). (2023). Cybersecurity workforce book: Building and sustaining the cybersecurity workforce. U.S. Department of Commerce. Retrieved from https://www.google.com/search?q=https://www.nist.gov/cybersecurity-workforce-book-latest-edition

National Cybersecurity Plan 2022. (2016, December 8). DICT. https://dict.gov.ph/wp-content/uploads/2017/04/NCSP2022.pdf

National Cybersecurity Plan 2023-2028. (2024, February). DICT.https://dict.gov.ph/national-cyber-security-plan

National Privacy Commission (NPC). (2022). *Annual Report on Data Breaches in the Philippines*. Quezon City: NPC.

Norona, M. I., & Aquino, F. A. (2021, March 7–11). Enhancing Cyber Security in the Philippine Academe: A Risk-Based IT Project Assessment Approach. 11th Annual

Pahi, D., et al. (2017). Exploring operational challenges in cybersecurity centers. *International Journal of Information Security Studies, 9*(3), 112–125.

Philippine Center for Investigative Journalism (PCIJ). (2021). *Cybersecurity and data breach cases in the Philippines*. Manila: PCIJ.

Philippine National Police (PNP). (2023). *Cyber Security Operations Center (CSOC) Operational Framework*. Quezon City: Directorate for ICT Management.

PNP DICTM. (2021). *Directorate for Information and Communication Technology Management Administrative and Operations Manual.* PNP DICTM, Camp Crame, Quezon City, Philippines.

Republic Act No. 10175 *Implementing Rules and Regulations*. (2015). DOJ Office of Cybercrime. https://cybercrime.doj.gov.ph/irr/

Purposive Sampling Guide. (2016). *Principles of purposive sampling in qualitative research*. [Publisher details].

Qualitative Methods Text. (2020). *Qualitative research methods: Foundations and applications*. [Publisher details].

Sahagun, J. C. (2024, March 10). Cybersecurity Threat: The Hacking of Websites of Owwa & Philippine Coast Guard. Metro Manila, Philippines. https://www.researchgate.net/publication/378853142

Scarfone, K., Benigni, D. and Grance, T. (2009), *Cyber Security Standards, Wiley Handbook of Science and Technology*

for Homeland Security, John Wiley & Sons, Inc., Hoboken, NJ. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153

Singapore Cyber Security Agency (CSA Singapore). (2021). *National Cybersecurity Strategy*. Singapore: CSA.

Sy, J. (2020). Data breaches and public trust in Philippine institutions. *Philippine Journal of Information Security, 12*(1), 33–47.

Tuscano, J. (2024, May). Cybersecurity Awareness Among Senior High School Students in District of Tanza: Basis for Cyber Education Program in Schools. https://www.researchgate.net/publication/381021932

World Economic Forum (WEF). (2024). *Global Risks Report 2024*. Geneva: WEF.