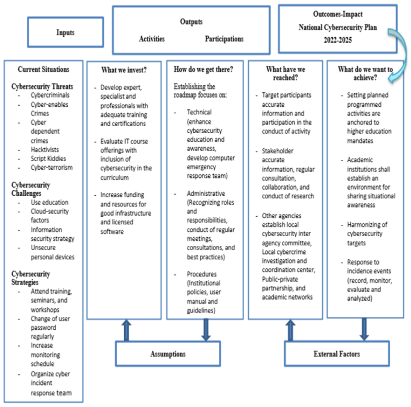
PHILIPPINE NORMAL UNIVERSITY
The National Center for Teacher Education

POLICY BRIEF SERIES

VOLUME 10 | ISSUE 2 | 2026 PRINT ISSN: 2984-9063 ONLINE ISSN: 2984-9071

# Developing the Cybersecurity Contextual Model in Philippine Higher Educational Institutions: Key Gaps and Strategic Actions for Education, Infrastructure, and Governance

***Noly M. De Ramos, Ed.D., Francisco D. Esponilla II., Ed.D., Jay-Ar G. Balauag, DIT***



**Current Situations**

**Cybersecurity Threats**
- Cybercriminals
- Cyber-enables Crimes
- Cyber dependent crimes
- Hacktivists
- Script Kiddies
- Cyber-terrorism

**Cybersecurity Challenges**
- Use education
- Cloud-security factors
- Information security strategy
- Unsecure personal devices

**Cybersecurity Strategies**
- Attend training, seminars, and workshops
- Change of user password regularly
- Increase monitoring schedule
- Organize cyber incident response team

**What we invest?**
- Develop expert, specialist and professionals with adequate training and certifications
- Evaluate IT course offerings with inclusion of cybersecurity in the curriculum
- Increase funding and resources for good infrastructure and licensed software

**How do we get there?**

Establishing the roadmap focuses on:
- Technical (enhance cybersecurity education and awareness, develop computer emergency response team)
- Administrative (Recognizing roles and responsibilities, conduct of regular meetings, consultations, and best practices)
- Procedures (Institutional policies, user manual and guidelines)

**What have we reached?**
- Target participants accurate information and participation in the conduct of activity
- Stakeholder accurate information, regular consultation, collaboration, and conduct of research
- Other agencies establish local cybersecurity inter agency committee, Local cybercrime investigation and coordination center, Public-private partnership, and academic networks

**What do we want to achieve?**
- Setting planned programmed activities are anchored to higher education mandates
- Academic institutions shall establish an environment for sharing situational awareness
- Harmonizing of cybersecurity targets
- Response to incidence events (record, monitor, evaluate and analyzed)

***HEI's Cybersecurity Program Logic Model***
***Source: De Ramos & Esponilla (2022)***
***Copyright Registration Certificate Number: 2025-01643-A***

Cybersecurity is becoming a major concern for schools and universities in the Philippines as they rely more on digital tools for everything from enrollment to synchronous and remote classes. The rapid shift online has opened them up to a growing number of cyber threats, especially with new, AI-powered attacks on the rise.

The biggest challenges are a lack of training, outdated technology, and limited budgets. Many schools just aren't doing enough—they don't regularly train students and staff on cybersecurity, nor do they enforce basic rules like strong password policies. Even though the threats are real and getting more dangerous, many institutions treat cybersecurity as a secondary concern. The recent data breach at Romblon State University and ongoing warnings from experts show that waiting isn't an option. It's clear that Philippine State Universities and Colleges (SUCs) must act now to protect their data, maintain trust, and ensure protecting institutional integrity, complying with national cybersecurity norms, safeguarding stakeholder trust, and enabling uninterrupted educational mission.

Recommended Citation:

De Ramos, N.M, Esponilla, F.D., & Mamauag, J.G., Developing the Cybersecurity Contextual Model in Philippine Higher Educational Institutions: Key Gaps and Strategic Actions for Education, Infrastructure, and Governance. *Policy Brief Series* 10 (2), pp. 1-6. Philippine Normal University Educational Policy Research and Development Office.

## Introduction

Philippine higher educational institutions are operating in a digital environment that is increasingly fraught with cyber risks. Recent surveys show that 84-85% of organizations in the Philippines experienced cybersecurity breaches in 2024, yet only 6% of organizations are assessed as having achieved a “mature” level of readiness (BusinessWorld, 2025).

In one headline case, Romblon State University was breached in April 2024 by a hacker group that exposed sensitive information of students and faculty, highlighting that even state colleges and universities (SUC) are not immune (Gil, 2024).

These trends underscore a pressing need for HEIs to shift from reactive to proactive cybersecurity postures. Key gaps include underinvestment in infrastructure, limited staff and student training, weak policies, and inadequate monitoring. Without a clear, coordinated framework to guide investment, training, policy development, and accountability, institutions remain vulnerable. A cybersecurity contextualized model-based approach offers structure: identifying what inputs (training, infrastructure, policies) are required, what activities these enable, and how those activities translate into outputs and measurable outcomes, thereby ensuring that resources are used effectively to build institutional resilience and protect sensitive data.

This study employed a multiple-case study design, utilizing purposive sampling of IT experts from selected Philippine State Universities and Colleges (SUCs) to investigate cybersecurity challenges. Data were gathered via structured interviews and subjected to thematic analysis, enabling the systematic identification of recurrent vulnerabilities and institutional practices. Notably, the original report's omission of precise details on the number of institutions and respondent demographics limits the findings to an exploratory, context-bound scope, precluding statistical generalizability.

The analysis identified systemic deficiencies across four primary domains: inadequate user awareness and behavioral practices, deficient cloud and cybersecurity strategies, lack of specialized governance positions, and inconsistent investments in defensive infrastructure. A proposed logic model framework delineates connections between requisite inputs (e.g., training, policies, technology), activities, and quantifiable outcomes; however, it remains conceptual, awaiting empirical validation.

## Key Issues

While many organizations in the Philippines are hit by cyberattacks, most are not prepared to handle them, with only about 6% considered to have "mature" cybersecurity (Newsbytes Philippines, 2025). This lack of readiness is also a major issue for higher educational institutions who face similar vulnerabilities. They often struggle with a lack of user training, weak policies, outdated technology, and a shortage of skilled staff. These weaknesses leave universities and colleges and DepED schools highly exposed to serious threats like data breaches, service interruptions, and damage to their public image.

**1. User Awareness, Education, and Behavior**

- Many faculty, staff, and students lack sufficient understanding of basic cybersecurity practices—password hygiene, account sharing, recognizing phishing, etc. “user education” as a major challenge.
- Older faculty members and non-IT users often share credentials or use generic/default logins. Such human errors increase vulnerability.
- Free WiFi and cloud-based tools are sometimes accessible only to personnel, IT students, and not all users, leaving many unaware of safe usage.

**2. Lack of Skilled Human Resources & Certifications**

- There is a shortage of trained cybersecurity professionals in academic institutions and across public/private sectors. HEIs often don’t have cybersecurity specialists; often, existing MIS or IT staff are expected to handle security among many other duties.
- Certifications are recognized as valuable but are under-prioritized due to high costs, limited budget, and lack of institutional support.

**3. Weak or Incomplete Institutional Policies & Strategy**

- Many SUCs do not have coherent and comprehensive information security strategies or roadmaps. Policies are often ad hoc, underdeveloped, or not enforced uniformly.
- Governance roles are unclear – there is rarely a dedicated security officer, formal oversight, or routine mechanism for policy review, incident response, or best practices sharing.

**4. Infrastructure, Technology & Cloud Security Gaps**

- The use of personal or unsecured devices (e.g., unpatched computers, default credentials) is common. SUCs often lack fully licensed and up-to-date security tools.
- Cloud usage is increasing, but many HEIs are not adequately guarded against cloud security risks. Some institutions haven’t prioritized cloud security due to costs.

**5. Underfunding & Resource Constraints**

- Budget limitations prevent HEIs from acquiring necessary security infrastructure, engaging in regular training, hiring or training dedicated staff, getting up-to-date tools, or pursuing certifications.

- Cybersecurity is often viewed as secondary to other institutional priorities until something bad happens. This reactive rather than proactive posture increases long-term risk.

**6. Internal Threats and Risk from Insider / Shared & Weak Credentials**

- Many of the threats come from inside: shared accounts, weak or generic logins, misuse of access by staff or students.
- System breach attempts, website defacements, malware, etc., are frequent, and internal users often account for a disproportionate share of security incidents.

**7. Lack of Monitoring, Incident Response & Measurement**

- HEIs often lack systematic monitoring (logs, access records), well-defined incident reporting mechanisms, or a way to assess whether policies and interventions are working.
- There is also often no regular evaluation or feedback loop to refine strategies or policies based on evolving threats.

**8. Rapidly Evolving Threat Landscape & Technological Complexity**

- Threats are growing more complex (malware, phishing, DDoS, insider threats, cloud misconfigurations, supply chain vulnerabilities) which require advanced tools and skills to counter.
- AI-related threats and alert fatigue are also emerging issues in the broader Philippine context.

**Key Findings and Policy Recommendations**

This study found that higher educational institutions are facing serious cybersecurity challenges including low levels of user education, weak cloud security, incomplete or poorly developed information security strategies, and widespread use of unsecured personal devices. These gaps limit institutions' ability to proactively defend against threats.

To help address these challenges, the study proposes a contextualized cybersecurity model or a framework that links what needs to be invested (training, technology, policy), what actions should be taken, and what outcomes should result so institutions can better plan, implement, and measure their cybersecurity efforts.

To enhance applicability, recommendations are prioritized by feasibility and urgency: immediate measures emphasize awareness training and policy enforcement; medium-term initiatives establish formalized governance; and long-term efforts cultivate technical capacity and resilience. This tiered approach facilitates efficient resource allocation toward enduring cybersecurity preparedness.

| Area | Findings |
|---|---|
| User Education & Awareness | Lack of regular training/orientation; older faculty sharing credentials; free WiFi usage info restricted only to IT students. |
| Security Strategy & Governance | No clear roadmap in many SUCs; no dedicated cybersecurity officer; budget limitations hinder certifications and proper protection. |
| Technological & Infrastructure Readiness | Some use firewalls, antivirus, IDS; but many institutions still use local systems, have minimal online systems, and no full MIS/infrastructure in place. |
| Exposure to Threats & Incidence | Frequent attempts at website defacement, script-kit attacks, misuse of shared accounts; internal accounts more often implicated than external hackers. |

**Policy Alternatives & Trade-offs**

| Option | Pros | Cons / Challenges |
|---|---|---|
| Increase training & awareness (for all staff, faculty, students) | Low cost; immediate impact on reducing human vulnerability; improved culture of security. | Requires continuous effort; possibly resistance; needs dedicated personnel/time. |
| Establish dedicated cybersecurity governance units/officer roles | Clearer accountability; focused strategy; better monitoring & incident response. | Budget constraints; lack of specialized human resources; time to institutionalize role. |

| | | |
|---|---|---|
| Upgrade infrastructure & adopt modern security tools | Stronger technical defenses (e.g. firewalls, IDS, endpoint protection); reduces attack surface. | Costly; maintenance & updating require ongoing resources; technical complexity. |
| Mandatory policy & standards (password policies, access control, incident logging, cloud security) | Sets minimum baseline; helps in compliance and consistency; easier monitoring. | Needs enforcement; compliance culture may be weak; oversight required. |

**Policy Recommendations**

The proposed HEIs Cybersecurity Contextualized Model provides a structured framework: identifying what inputs (training, resources, governance) are needed, what actions (policy creation, monitoring, incident response) should follow, and what outcomes (reduced breaches, better preparedness, stronger culture) should result.

By adopting this model, HEIs can bridge the gap between current vulnerabilities and desired resilience. The model helps ensure that every investment and policy is aligned, measurable, and accountable—transforming cybersecurity from a reactive issue into a planned, institution-wide priority.

1. Implement mandatory cybersecurity training, orientation, and certification for faculty, administrative staff, and students.

2. Designate information security officers in each HEIs, with clear responsibilities for monitoring, policy enforcement, and incident response.

3. Develop a national/regional/institutional roadmap (in collaboration among DICT, CHED, DepEd, PASUC, PNP, NBI) for cybersecurity readiness across HEIs, including benchmarks for infrastructure, governance, and awareness.

4. Allocate dedicated funding for cybersecurity infrastructure, software licenses, and regular audits.

5. Formulate and enforce institutional policies on password management, account sharing, cloud security usage, endpoint protection, and incident logging.

6. Encourage public-private partnerships to provide discounted or shared cybersecurity services, technical support, and capacity building.

**Conclusion**

Strengthening cybersecurity in HEIs is no longer optional—it is essential for institutional integrity, continuity, and trust. By focusing first on user education, governance, and foundational policies, and by allocating resources strategically, HEIs can significantly reduce vulnerabilities. Collaboration among HEIs and with government agencies will help in scaling solutions and ensuring sustainability.

The HEIs Cybersecurity Contextualized Model is not just another theory—it is a necessary, practical framework that can meaningfully strengthen security across Philippine higher educational institutions. The model addresses the very gaps that leave HEIs exposed: lack of user training and awareness; vague or absent policy roles; underinvestment in infrastructure; poor monitoring; and weak incident response. By clearly defining what inputs (training, technology, governance) are needed, mapping actionable strategies (seminars, policy enforcement, access controls), and tying them to measurable outcomes (fewer breaches, stronger policies, operational resilience), the HEIs cybersecurity contextualized model converts nebulous challenges into structured, accountable action. Moreover, this model dovetails with broader national efforts, such as the National Cybersecurity Plan 2023–2028 and aligns with global standards for cybersecurity governance. For instance, the government's commitment to minimum information security standards, increased technical skill development, and awareness campaigns shows strong momentum.

Implementing the HEIs model can help leverage this momentum: not only to comply with regulatory expectations but to build internal capacity, reduce risks proactively, and protect sensitive data and institutional reputation.

Ultimately, HEIs adopting this contextualized model are investing in long-term institutional health. Better security means fewer disruptions, stronger trust among students, faculty, staff, and external partners; less financial loss from breaches; and the ability to embrace digital transformation with confidence. Institutions that fail to act—or that act too slowly—risk exposing themselves to avoidable harms. In a rapidly evolving threat environment, this framework is an essential blueprint: coherent, measurable, and aligned with both local context and national cybersecurity ambitions.

## REFERENCES:

Asia Foundation. (2022). Cybersecurity in the Philippines: Global context and local challenges. The Asia Foundation. https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf

BusinessWorld. (2025, January 23). Over 80 PHL organizations hit by cybersecurity breaches in 2024. BusinessWorld Online. https://www.bworldonline.com/technology/2025/01/23/648190/over-80-phl-organizations-hit-by-cybersecurity-breaches-in-2024/

Cyberint. (2024). Philippine threat landscape report 2024-2025. Cyberint. https://e.cyberint.com/hubfs/Philippine%20Threat%20Landscape%20Report%202024.pdf

De Ramos, N. M., & Esponilla II, F. D. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education (IJERE), 11(3). https://doi.org/10.11591/ijere.v11i3.22863

Dharmaraj, S. (2024, October 1). Building resilience: The Philippines enhances cybersecurity. OpenGov Asia. https://opengovasia.com/2024/10/01/building-resilience-the-philippines-enhances-cybersecurity

Gil, M. (2024, April 30). Romblon State U assesses data breach after website hacking. Philippine News Agency. https://www.pna.gov.ph/articles/1223765

Manila Bulletin. (2024, May 3). DICT highlights the shortage of cybersecurity experts in the Philippines. Manila Bulletin. https://mb.com.ph/2024/5/3/dict-highlights-shortage-of-cybersecurity-experts-in-the-philippines

National Privacy Commission. (n.d.). Data security. https://privacy.gov.ph/data-security/

Newsbytes Philippines. (2025, May 16). Study: PH cybersecurity readiness remains low at 6. Newsbytes. https://newsbytes.ph/2025/05/16/study-ph-cybersecurity-readiness-remains-low-at-6

Omorog, C. D., & Medina, R. P. (2020). Internet security awareness of Filipinos: A survey paper. arXiv. https://arxiv.org/abs/2012.03669

SunStar Publishing Inc. (2025, May 9). PH cybersecurity is still weak amid rising AI threats. SunStar. https://www.sunstar.com.ph/cebu/ph-cybersecurity-still-weak-amid-rising-ai-threats

Unisys. (2019, March 27). The Philippines shows the highest level of concern over security. Unisys Security Index. https://www.unisys.com/news-release/ph-the-philippines-shows-the-highest-level-of-concern/

## Declaration

We declare that the content of this research is our own original work, except where we have used the work of others, but provided proper acknowledgment. In preparing and improving this document, we used artificial intelligence (AI) tools, specifically ChatGPT, Gemini and Perplexity solely for checking grammar and enhancing sentence structure. We want to be clear that we did not use AI to generate ideas, create content, or analyze and interpret data.

All intellectual contributions, analyses, and conclusions in this paper are our own. Our use of AI adheres to all institutional policies on academic integrity. we take full responsibility for the accuracy, originality, and ethical compliance of this research.

## ABOUT THE AUTHORS

**Dr. Noly M. De Ramos**, is an academic and extension practitioner engaged in higher education policy, curriculum development, and community governance. His work supports evidence-based decision-making through research-informed programs aligned with quality assurance standards, sustainable development goals, and inclusive digital transformation in local communities.

Contact No: 09228897619.
Email: deramos.nm@pnu.edu.ph

**Dr. Francisco D. Esponilla II** is a dedicated academic and active researcher committed to advancing knowledge through rigorous scholarly work. He is engaged in research, teaching, and professional service, with a strong focus on contributing meaningful insights to his field and supporting institutional and academic development.

Contact No.: 0999-977-7764,
Email: Francisco_esponilla@tup.edu.ph

**Dr. Jay-Ar G. Balauag** is an Assistant Professor at Philippine Normal University North Luzon and a Doctor of Information Technology graduate. He has teaching experience in Information Assurance and Security, System Automation, and System Integration at the University of La Salette, Inc., areas closely aligned with cybersecurity.

Contact No. **09762128536**
Email**:** balauag.jg@pnu.edu.ph

## The PNU Educational Policy Research, and Development Office

The EPRDO is a specialized research center in the University focused on policy research and studies on teacher education. It is established to provide research-based policy recommendations to policy makers. It also serves as the clearing house for all data relevant to teacher education in the Philippines and beyond.

### Vision

The Philippine Normal University through the EPRDO aims to be an innovation hub of teacher education research and educational policy studies.

### Mission

To strengthen the culture of excellence in teacher education research and educational policy studies.

### Objectives

The EPRDO shall manage the University's research production, enhance human resource capabilities, and share expertise to other Teacher Education Institutions (TEIs) in the area of teacher education research

### Strategies

1. Establish and maintain a web-based university research portal that facilitates automated research management systems, and which also serves as the database of teacher education policies and teacher education research in the country and Southeast Asia.
2. Share research expertise and competence in teacher education research with other TEIs throughout the country;
3. Develop and disseminate the University research agenda
4. Design and implement the research capability program for faculty and staff;
5. Manage University's research production particularly the conduct of educational policy studies in education and teacher education; and
6. Serve as the implementing arm for research incentives and research ethics review.

### Values

SYNERGY (Working collaboratively as a team)
EFFICIENCY (Delivering research services efficiently)
EXCELLENCE (Achieving high quality research outputs)
PRODUCTIVITY (increasing research production of the University)

The **Policy Brief Series** aims to provide observations, analyses, and insights by PNU faculty and researchers on various educational policy issues. The views contained in the policy briefs are those of the authors and do not necessarily represent the official views of the University.

The **Policy Brief Series** is published monthly by the **Philippine Normal University Educational Policy Research and Development Office** (PNU-EPRDO). The PNU-EPRDO oversees the editing, compiling, and printing of the policy brief.

*Address*
Room 205, Pedro Orata Hall
Philippine Normal University, Manila, Philippines 1000

https://www.facebook.com/pnueprdo