From Compliance to Resilience: Assessing Cybersecurity Maturity of State Universities and Colleges in the Philippines

Dr. Mark L. Flores
College of Computing Studies, Western Mindanao State University, Zamboanga City, Philippines
mark.flores@wmsu.edu.ph

ABSTRACT

This study evaluated the cybersecurity maturity of six State Universities and Colleges (SUCs) in the Zamboanga Peninsula. Using surveys and interviews, maturity was assessed across five domains: information security, strategy, policy, training, and incident response. Findings showed SUCs were moderately mature in cybersecurity (3.21/5), strongest in information security but weakest in training and incident response. Policies existed, but enforcement and incident readiness lagged, especially where ICT experience and training were lacking. Importantly, the results underscored that demographics like age or sex had no bearing on security maturity; rather, targeted, repeated professional development was decisive. Interviews revealed similar difficulties in governance and funding, matching global trends. The study suggests that focus should be on governance-driven strategies, structured awareness programs, stronger enforcement mechanisms, and tested incident-response plans to help SUCs move beyond basic compliance to real resilience.

Keywords: Cybersecurity maturity, Compliance–resilience approach, Higher education institutions, Policy enforcement, Philippines

INTRODUCTION

Digitization has revolutionized universities and colleges' teaching, learning, and operations, but it also brings increased cybersecurity challenges. Institutions of higher learning are vulnerable to cybercriminals due to the sensitive information they hold, including student records, research findings, and financial details. The recent assessments show that HEIs have been deploying various ICT security tools and techniques, but the implementation is scattered and inconsistent [1], [4]. Moreover, studies into security education and training methodologies-such as traditional seminars, virtual reality, and augmented reality-have begun to explore how immersive and innovative approaches can enhance awareness and skills transfer to faculty and student populations [5]. Furthermore, systematic maps of practices in IT governance show that cybersecurity in higher education institutions is often compromised by very weak institutional structures and limited accountability mechanisms [2].

Studies highlight that HEIs face persistent threats such as phishing, ransomware, and data breaches, but responses are frequently reactive rather than proactive [3], [4]. Ramos and Francisco [7] point out that in the Philippines, cybersecurity programs at colleges and universities are still taking shape. Progress is often slowed by a lack of resources and varying levels of commitment across different schools.. These findings echo international literature that identifies common challenges, including lack of integrated governance, minimal training, poor enforcement of policies, and untested incident-response mechanisms [15], [16].

In the Philippines, the Data Privacy Act of 2012 (RA 10173) mandates the protection of personal and institutional data, prompting State Universities and Colleges (SUCs) to adopt baseline measures. However, simply meeting regulatory requirements isn't the same as being resilient. Compliance ensures policies and technical protections are implemented for rules but true preparedness is only about what to prepare for, how to endure, and retrace the steps taken back with regard to unexpected incidents. Good leaders, very good staff, and practices that have been carefully tested are needed [19], [20]. Recent reviews of cybersecurity maturity assessments further accentuate the importance of sector-specific frameworks showing that resilience requires specific models reflecting organizational context rather than generic compliance checklists [6]. For higher education institutions everywhere, closing the gap between compliance and resilience is crucial—and for Philippine SUCs, it's even more urgent given their challenges with funding, organization, and people.

This study addresses that gap by evaluating the cybersecurity maturity of six SUCs in the Zamboanga Peninsula. Using surveys and interviews, maturity was assessed across five domains—information security, strategy, policy, training, and incident response—and examined both quantitative and qualitative indicators. The aim is to determine the extent to which SUCs remain compliance-oriented and what measures are needed for them to transition toward resilience-oriented frameworks.

This study was guided by the following research questions:

1. What is the cybersecurity maturity level of SUCs in the Zamboanga Peninsula on the domains of information security, strategy, policy, training, and incident response?

2. How does the implementation of cybersecurity practices in SUCs differ when respondents' data are grouped according to age, sex, ICT experience, and training exposure?
3. What institutional gaps and challenges affect the effective enforcement of policies, governance strategies, and incident-response mechanisms in SUCs?
4. How can SUCs strengthen their cybersecurity posture to transition from compliance-oriented practices to resilience-oriented frameworks?

Theoretical and Conceptual Framework

Theoretical Framework

This study was anchored in theories of cybersecurity maturity**,** IT governance in higher education**,** and information security awareness**.**

Maturity assessment frameworks provide universities with a structured path for evaluating cybersecurity preparedness. Almomani et al. [9] found that many universities focus on complying with minimal occupational health and safety standards rather than pursuing overall resiliency. Ulven and Wangen [16] found that institutions meet specifications but rarely achieve true resilience despite systematic risk assessments.

Research on IT governance clarifies the internal mechanisms needed for effective cybersecurity implementation. Meçe et al. [2] highlighted the critical roles of steering committees, sufficient funding, and clearly defined responsibilities in higher education institutions. Moroccan case studies demonstrated that tailoring governance structures to unique contexts enhances cybersecurity outcomes [10].

Theories on human behavior and awareness emphasize that true resilience depends on technical solutions, policies, and everyday user practices. Lebek et al. [17] found that continuous training and awareness campaigns foster secure user behaviors. Alnajim et al. [5] explored the potential of immersive learning tools to strengthen cybersecurity education and training, especially in academic settings.

Policy research recasts cybersecurity as a spectrum between compliance and resilience. Fouad [19] argued that higher education institutions globally prioritize compliance but often lack resilience. Kautwima et al. [18] reported inconsistent policy enforcement, creating gaps in overall implementation. This insight is relevant to Philippine SUCs, where adherence to the Data Privacy Act (RA 10173) drives compliance efforts but doesn't automatically confer resilience [8].

Conceptual Framework

This study investigated how Philippine state universities and colleges (SUCs) address cybersecurity maturity across five interconnected domains.

1. Information Security: It is a domain dealing with the technical safeguards for digital assets like encryption, user authentication, endpoint security, and most of all periodic penetration-testing to discover vulnerabilities [1], [4].
2. Strategy: The research focuses on the indicators such as roadmaps and measurable conclusions to know if these institutions have them, as well as the level of leadership involvement in cybersecurity planning and oversight [15].
3. Policy: This study assessed, not only whether such ICT and data privacy policies existed, but also whether they were monitored and effectively enforced within the institution [18]..
4. Training: Covering all levels and quality of cybersecurity training, from general awareness campaigns to specific, role-based workshops and consideration for newer learning tools-such as virtual or augmented reality-that will further bolster security skills and user-safe behavior [5], [17].
5. Incident Response: Conclusively, the study evaluated the preparedness of the universities in responding to cyber incidents by assessing whether there was an incident response plan and whether it was tested periodically, and also the efficacy or reliability of swift escalation and recovery processes [16], [19].

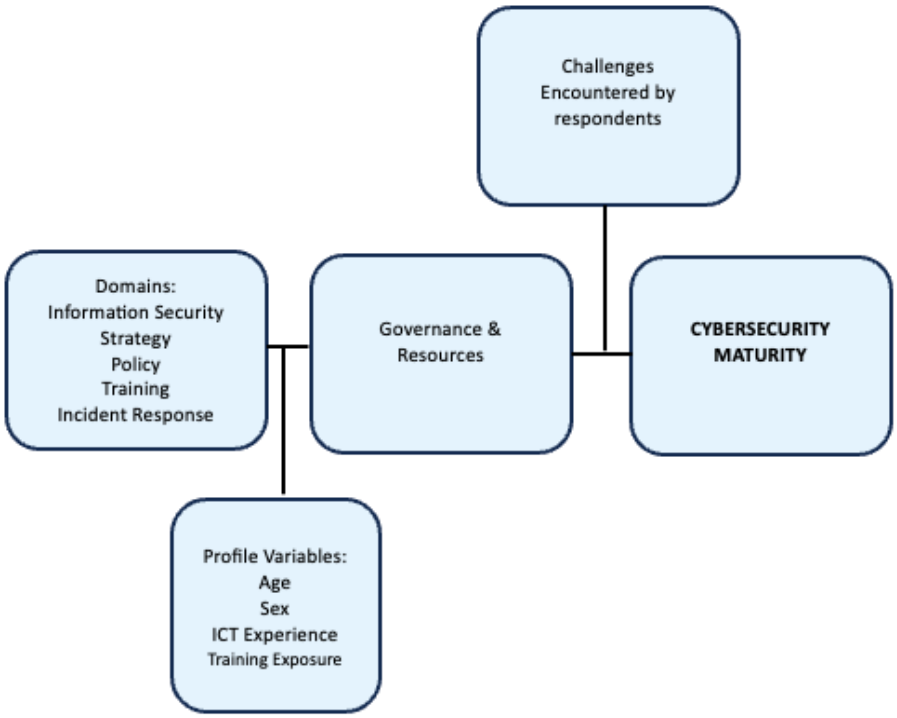


Figure 1. Conceptual Framework of the Study.

The framework illustrates how profile variables (age, sex, ICT experience and training exposure) influence the five domains of cybersecurity maturity: Information Security, Strategy, Policy, Training, and Incident Response. These domains are moderated by governance and institutional resources (e.g., steering committees, policy enforcement, budget allocation), which serve as enablers or barriers. The outcome is the overall cybersecurity maturity level of SUCs, positioned on a compliance to resilience approach

The independent variables included profile variables (age, sex, ICT experience, training exposure), which influence domain maturity. The mediating factors were governance arrangements and resources [2], [10]. The dependent variable was the overall cybersecurity maturity score, interpreted along the compliance–resilience approach [9], [19].

METHODOLOGY

Research Design

The study employed a descriptive quantitative design supplemented by semi-structured qualitative interviews. Mixed-method approaches have been recommended for information-security research in organizational settings because they combine the measurement precision of surveys with the contextual depth of interviews, enabling a fuller understanding of governance and practice gaps [14].

Locale and Participants

The research was carried out across six State Universities and Colleges (SUCs) in the Zamboanga Peninsula, anonymized as SUC A–F to preserve confidentiality. A total of 63 respondents participated; these were ICT personnel and Computer Science/IT faculty who were directly involved in managing institutional ICT infrastructure and security. Participants were selected purposively to ensure information-rich respondents with domain expertise [11].

Research Instrument

A structured questionnaire was developed to measure five domains: Information Security, Strategy, Policy, Training, and Incident Response. Items used a five-point Likert scale (1 = Not Evident to 5 = Very Evident). The instrument was reviewed by three subject-matter experts for content validity and pilot tested. Internal consistency was assessed using Cronbach's alpha, which yielded a reliability coefficient of $\alpha = 0.83$, consistent with best practice in instrument reliability reporting [13].

To complement the survey, semi-structured interviews with ICT coordinators and selected faculty were conducted to uncover institutional challenges (e.g., budget constraints, policy enforcement, privacy compliance) that could not be fully captured through the quantitative instrument. Interview data were analyzed using thematic analysis, following an established stepwise approach to coding and theme development [12].

Data Collection Procedure

Data were collected in Academic Year 2021–2022. Prior to participation, respondents were provided a study information sheet and gave informed consent. Surveys were administered electronically. Interviews were conducted virtually and audio-recorded with permission. All data were anonymized before analysis.

Data Analysis

Quantitative data were analyzed using SPSS. Descriptive statistics (mean, standard deviation, frequency distribution) summarized the status and extent of cybersecurity practices. t-test and one-way ANOVA were used to examine differences across profile variables (e.g., age, sex, years of ICT experience, number of trainings); post-hoc tests were reported when appropriate. Interview transcripts were coded and analyzed thematically to identify recurring patterns and institutional barriers; this triangulation strengthened the interpretation of survey findings [12].

Ethical Considerations

The study secured ethical approval from the host university's Research Ethics Committee. Participation was voluntary and confidential; no personally identifiable information was published. Data handling followed the Data Privacy Act of 2012 (RA 10173) and institutional data protection practices.

RESULTS

Overall maturity: status and extent

The computed overall weighted mean for the five domains of cybersecurity management was 3.21/5.00, interpreted as Moderate**.** Table 1 presents the domain-wise scores.

Table 1. Weighted mean scores of cybersecurity domains

Domain	*Weighted Mean*	*Verbal Interpretation*	*Rank*
Information Security	3.45	Moderate	1
Policy	3.36	Moderate	2
Strategy	3.12	Moderate	3

Domain	*Weighted Mean*	*Verbal Interpretation*	*Rank*
Incident Response	3.08	Moderate	4
Training	3.05	Moderate	5
Overall	**3.21**	**Moderate**	

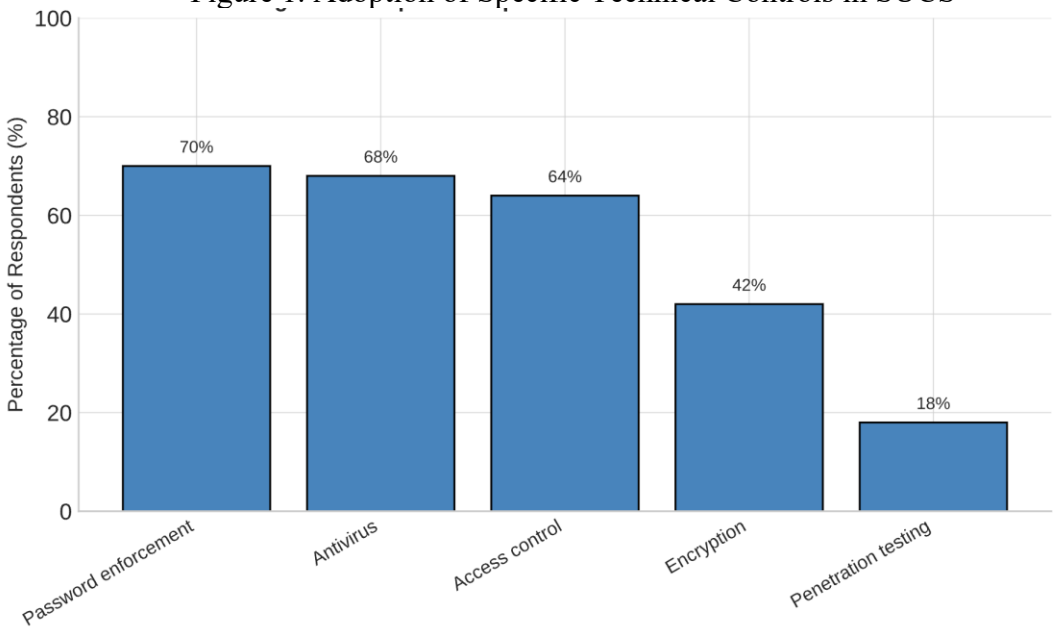
The table showed that Information Security ranked highest, reflecting emphasis on technical controls (e.g., antivirus, passwords), while Training and Incident Response ranked lowest. This imbalance suggested that SUCs focused on technical compliance while underestimating human and procedural resilience. Such imbalance is also reported in global HEIs, where compliance measures dominate while governance and training lag behind [15], [16].

Domain-by-domain findings

Information security (technical controls)

Respondents indicated high adoption of basic controls: 70% confirmed consistent password enforcement, 68% antivirus use, and 64% access control mechanisms. However, only 42% reported data encryption, and a mere 18% confirmed routine penetration testing.

Figure 1. Percentage of respondents reporting adoption of specific technical controls



The research highlights the dramatic contrast between the most basic types of security tools and the adoption of more advanced and extensive resilient practices among SUCs. Universities in this category must meet at least the

more indirect commands of a basic security set; however, they often do not achieve a very in-depth level that would provide true resilience. This pattern is congruent with Ulven and Wangen's [16] global observation that higher education institutions basically do not pay attention to a systematic vulnerability management framework, hence exposing themselves to risk.

In practical terms, it means SUCs are somewhat able to protect themselves against day-to-day threats such as generic viruses with basic antivirus solutions. They are, however, exposed to more sophisticated threats of advanced persistent threats or ransomware attacks that call for solid defense mechanisms such as encryption and continuous penetration testing. Lacking these advanced means of protection, institutions would remain especially vulnerable to such targeted attacks directed mainly at compromising research data or incapacitating vital academic operations.

Strategy and governance

Only **35%** of respondents stated their SUCs had a documented cybersecurity strategy, while **65%** admitted no such roadmap.

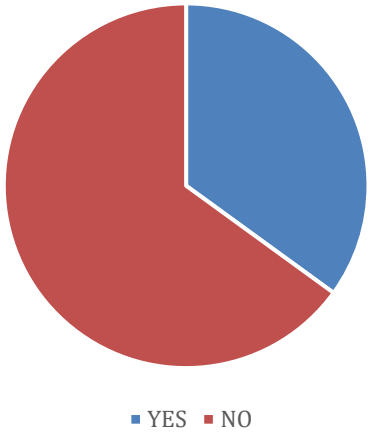


Figure 2. Existence of Documented Cybersecurity Strategies in SUCS

The absence of institutional strategies meant that cybersecurity initiatives were reactive rather than proactive. Cheng and Wang [15] stressed that leadership and KPIs are critical to making cybersecurity a sustainable institutional priority. Without strategies, SUCs risk aligning cybersecurity only with ICT teams, neglecting integration with finance, HR, and administration.

The absence of strategies also implied weak budget advocacy. Without a roadmap, ICT heads struggle to argue for cybersecurity funds, as they lack

KPIs to demonstrate progress or risks. This institutional blind spot explains why budget repeatedly emerged as a barrier in interviews.

4.2.3 Policies and enforcement

Policy presence was rated higher **(**mean = 3.54**)** than policy enforcement **(**mean = 2.88**)**, as shown in Table 2**.**

Table 2. Policy presence vs. enforcement

Indicator	*Mean Score*	*Interpretation*
Policy presence	3.54	Moderate
Policy enforcement	2.88	Low–Moderate

The disparity between policy and practice, as Kautwima et al. [18] found, persists, and this very inequality highlights it. The respondents perceived written policies-like those that guided ICT use and privacy compliance-but they noticed the absence of systematic audits or any sanctions that could enforce the observance of these rules.

Hence there developed a "false sense of safety": while documented policies suggested of institutional compliance, end-users actually often circumvented these policies. This discrepancy between formal guidelines and everyday conduct weakened the resilience of the institution and raised the level of risk of its noncompliance with RA 10173 (Data Privacy Act).

Workforce capacity, awareness, and training

Statistical tests showed significant differences in implementation based on ICT experience and training. Respondents with ≥5 years ICT experience scored higher **(**mean = 3.45**)** than those with <5 years **(**mean = 2.98, p = 0.021). Similarly, respondents with **≥3** cybersecurity trainings scored higher (mean = 3.62) than those with none (mean = 2.84, p = 0.017).

Table 3. Differences in implementation scores by training and experience

Group	*Mean Score*	*p-value*	*Interpretation*
< 5 years ICT exp.	2.98		Lower
≥ 5 years ICT exp.	3.45	0.021	Higher
No trainings	2.84		Lower
≥ 3 trainings	3.62	0.017	Higher

The findings reinforced and complemented the conclusions of Lebek et al.[17], which stress that awareness and training are vital to the development

of secure behavior in organizations. Importantly, the evidence demonstrates that systematic training is a "force multiplier": with scant resources, SUCs can significantly improve their cybersecurity posture through an investment in the ongoing development of their staff.

Most importantly, the study showed that factors like age or sex had no influence on security maturity. Rather, the key was the repeated delivery of targeted professional training, which stands out as a viable and cost-efficient option for toughening institutional defense.

Incident detection and response

Only 22% of respondents reported having a formal incident-response plan (IRP), and just **8%** confirmed testing it in the past year.

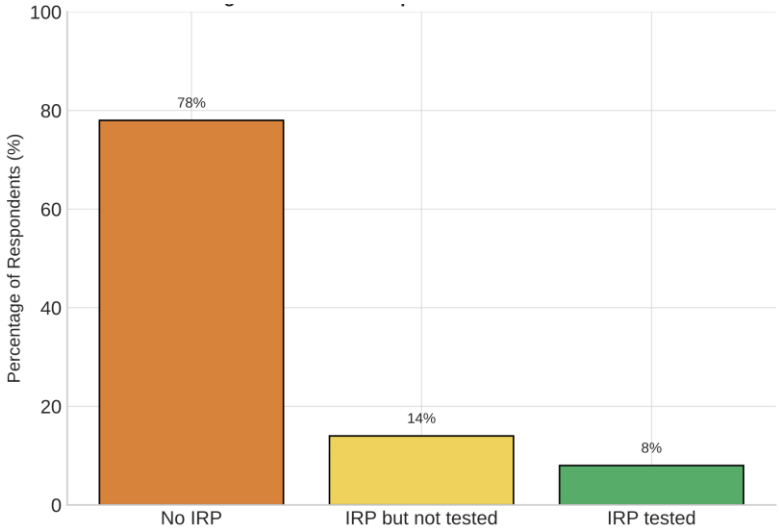


Figure 3. Incident-response Readiness in SUCs

According to the findings, although a small portion of institutions responded with incident response plans (IRPs), they were not truly ready for any incidents. The IRPs cited by Fouad [19] are beneficial for testing and regularly maintained in higher education because they can have a direct impact on the reputation and credibility of the institutions when any interruption occurs to their critical systems, such as in learning management platforms and research databases.

Interviews further revealed that many of the ICT staff were ill-informed about the procedures to escalate emergent incidents, at the same time causing an uncertain climate on whether or not the breaches were required to be reported to management or other external authorities. This condition that lacks definite escalation protocols has great indications of risk, since delays in responding and communicating breaches may amplify very much any resulting damages, hence undermining the capacity to contain and recover from cyber incidents.

Drivers and barriers

Interview themes, summarized in Table 4, reinforced the survey findings.

Table 4. Thematic issues from interviews

Theme	*Evidence from SUCs*	*Literature link*
Leadership priority	Cybersecurity often left to ICT teams only	[15], [19]
Budget constraints	Insufficient allocation for tools & training	[16]
Human capacity	Overburdened ICT staff with multiple responsibilities	[19]
Policy–practice gap	Policies exist but weak enforcement	[18]

The convergence of quantitative and qualitative results painted a consistent picture: SUCs faced not just technological gaps, but also organizational, financial, and cultural barriers. Importantly, these barriers were not unique to Philippine HEIs — they echoed findings across Africa, Europe, and the Middle East [15]–[19]. This reinforced that SUCs needed a hybrid framework combining governance reforms, cultural change, and affordable technical measures.

DISCUSSION

This study found through the quantitative and qualitative integration that of the six SUCs examined, compliance rather than real resilience was the focus. Though some formal policies and technical controls are expressed and in theory exist, their enforcement would appear weak; governance structures are not uniformly integrated; capacity-building is not always conducted; and incident-response mechanisms' effectiveness is hardly tested. This mirrors worldwide trends in which higher education institutions are deemed to somehow plateau or cease development after at least achieving minimum compliance, owing to the notion that resilience resides somewhere in the nebulously defined terrain of greater governance, human, and experiential practices [15], [16], [19], [20].

The study’s findings highlight four interdependent priorities for SUCs: (1) governance, (2) capacity building, (3) policy enforcement, and (4) incident-response testing. Each priority is practical, actionable, and grounded in existing literature:

Governance: Properly strategized and visible in leadership levels, effective cybersecurity has policies that flow into standards, procedures, and resource allocation to achieve long-term funding for sustaining outcomes. Evidence from institutional case studies demonstrates their associated progress

regarding implementation maturity with executive sponsorship (such as steering committees led by top-level administrators); formal KPIs; specific cybersecurity budgets [15], [20]. Such forums for governance would lead SUCs to form an executive-level governance forum, publish a clear cybersecurity roadmap linked to risks and resources, and track a concise set of key metrics (for instance, time-to-patch, backup validation rates, and multi-factor authentication adoption). Best practices talk about well-structured charters, meeting cadences, and escalation protocols that are very rigid [21]. Beginning with a 12-month roadmap and KPI dashboard reviewed quarterly could establish the link from the strategic plan to measurable security outcomes.

Capacity Building: Regularly structured training is, by far, the most scalable and cost-effective method available to build a culture of institutional security and improve operational effectiveness. The literature is quite emphatic that continuous, job-related and hands-on training (including simulation and immersive experiences where possible) would produce improvements more meaningful than one-off lectures [5], [17], [22]. This means that in SUCs, tiered pathways are to be taken for training- general awareness for all, advanced modules for ICT roles, and practical exercises for incident teams. Monitoring participation as a KPI and yearly updating the materials while inserting some occasional simulations or gamification may drive engagement and retention [22].

Policy Enforcement: Combining behavioral reinforcement and management oversight will help bridge the enduring gulf between policy and practice in our daily lives. While research has shown limits to the effectiveness of sanctions, a positive outcome is achieved via a combination of communication, fairness, and a compliance culture that offers support [23]. In practical terms, it is best to couple the scheduling of annual audits and a system of automated checks, which are transparent and objective, with sanctions that are much clearer and more proportionate. Remedial training and clarification of role expectations may also serve to bring down violations [24]. Most importantly, interlinking compliance data with governance reviews accelerates improvement.

Incident Response Testing: Practicing incident-response plans regularly must become a recurring exercise to effect rapid containment and recovery. Evidence exists whereby tabletop exercises and after-action reviews significantly augment preparedness, clarify roles, and surface hidden dependencies [25],[26],[and 8]. Lightweight IRP templates and annual exercises with senior leaders, logging action points, and updating plans based

on lessons learned are paramount for SUCs. The collaboration with external partners such as regional CERTs further enhances maturity.

International evidence confirm the empirical findings-the rather low Cybersecurity scores; the value of training; and the gap between policy and practice-that organizational factors such as governance and culture matter as much as technical controls [15]-[17], [19]-[26]. Helpful to the SUCs would be an explicit four-part action that would be: (1) secure leadership support with a prioritized roadmap; (2) institutionalize KPIs and monitoring; (3) roll out multi-level training; and (4) conduct periodic exercises and update incident response plans. This sequence will create easy wins, build momentum, and thus link resources and strategy to very tangible improvements in security and privacy readiness.

CONCLUSION

The analysis shows that the six State Universities and Colleges (SUCs) of Zamboanga Peninsula have made tangible efforts in improving their cybersecurity safeguards but there are still significant existing vulnerabilities. These institutions have established basic technical precautions and a minimal number of policy frameworks, but there are significant gaps remaining in the continued analysis of strategic planning, enforcement of policy, activities for capability building, and preparedness for incident response. Most actions lack definitive cybersecurity strategies, while policies seem to exist merely on paper and poorly implemented within the institutions. Some training of staff and students was sparse, yet such training was not well-specific to roles; very rare incidents occurred in applying or reassessing the incident-response mechanisms. These findings resonate with a global trend impacting higher education, as institutions remain technically compliant but otherwise seldom embrace more resilient practices[3, 4, 15, 16, 19].

The study establishes once again, with human and organizational factors as crucial determinants in the maturity of any organization in cybersecurity, that institutional awareness, targeted training, and direct experience are foremost in enabling secure user behavior, affirming the findings of the global studies that address the impact of individual and collective actions on institutional cybersecurity [5], [17]. The presence of well-defined governance structures (active cybersecurity committees with clear budget allocation) was critical for the conversion of policy into practice, in alignment with evidence from studies of effective IT governance in higher education [2], [10], [20]. Essential in the experience of the studied SUCs is that compliance is however only one

important, not the only, building stone; resilience depends on anchoring in governance, continual professional development, and actual policy implementation, and on regular testing of response capabilities in a realistic manner.

The study recommends that institutional leaders undertake cyber governance improvements by setting commitments to strategies, significant Key Performance Indicators reporting measure, and assure ongoing and sufficient funding. Research has shown that these frameworks demonstrate strong relationships with organizations' readiness for operations and resilience [10] , [15], [20]. Also, SUCs should practice periodic, position-relevant cybersecurity training courses that promote awareness and compliance through the use of creative mediums, such as immersive technology (VR or AR) or simulations [5],[17].Policies should be developed, monitored with compliance, and held accountable through routine audits and consequences of action (proportionate accountability), in order to bridge the policy-practice gap that greatly impedes maturity [18],[19].Another major consideration is having and regularly updating and testing incident-response plans, which distinguish those organizations that can build resilience from those that rely upon the application of an operational process [16],[19].Finally, exposing faculty, staff, and students themselves to concepts of cybersecurity in the formal curriculum, new faculty orientation, and professional development will begin at, and throughout the institution, a culture of faculty engagement and resilience to a cyber event or loss [15],[20].Altogether, these actions present a concise and pragmatic lens to elevate SUCs from basic compliance to one with a culture of ongoing cybersecurity resilience.

References:

[1] M. Nuñez, X.-L. Palmer, L. Potter, C. J. Aliac, and L. C. Velasco, “ICT security tools and techniques among higher education institutions: A critical review,” *Int. J. Emerg. Technol. Learn. (iJET)*, vol. 18, no. 15, pp. 4–22, 2023.

[2] E. K. Meçe *et al.*, “Governing IT in HEIs: Systematic mapping review,” *Bus. Syst. Res. J.*, vol. 11, no. 3, pp. 93–109, Nov. 2020.

[3] J. Ulven and G. Wangen, “Cybersecurity in higher education institutions: Threats and practices,” *Inf. Secur. J.: A Glob. Perspect.*, vol. 31, no. 2, pp. 75–88, 2022.

[4] A. Alotaibi, “Cybersecurity challenges and solutions in higher education institutions: A literature review,” *IEEE Access*, vol. 9, pp. 160233–160249, 2021.

[5] A. Alnajim, S. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, “Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches,” *Symmetry*, vol. 15, no. 12, Art. 2175, 2023, doi: 10.3390/sym15122175.

[6] A. Brezavšček and A. Baggia, “Recent trends in information and cyber security maturity assessment: A systematic literature review,” *Systems*, vol. 13, no. 1, 2025, doi: 10.3390/systems13010052.

[7] J. Ramos and R. Francisco, “Cybersecurity program for Philippine higher education institutions: A multiple-case study,” *J. Educ. Technol.*, vol. 9, no. 3, pp. 112–125, 2022.

[8] National Privacy Commission, *Implementing Rules and Regulations of Republic Act No. 10173, the Data Privacy Act of 2012*. Manila, Philippines: National Privacy Commission, 2016.
[9] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, Art. e703, 2021, doi: 10.7717/peerj-cs.703.
[10] C. Abdelilah, S. Ahriz, K. El Guemmat, and K. Mansouri, "Implementation of suitable information technology governance frameworks for Moroccan higher education institutions," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 3, pp. 3116–3126, 2024, doi: 10.11591/ijece.v14i3.pp3116-3126.
[11] L. A. Palinkas, S. M. Horwitz, C. A. Green, J. P. Wisdom, N. Duan, and K. Hoagwood, "Purposeful sampling for qualitative data collection and analysis in mixed method implementation research," *Adm. Policy Ment. Health Ment. Health Serv. Res.*, vol. 42, no. 5, pp. 533–544, 2015, doi: 10.1007/s10488-013-0528-y.
[12] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.
[13] M. Tavakol and R. Dennick, "Making sense of Cronbach's alpha," *Int. J. Med. Educ.*, vol. 2, pp. 53–55, 2011.
[14] A. Zanke, T. Weber, P. Dornheim, and M. Engel, "Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments," *Comput. Secur.*, vol. 144, Art. 103938, 2024, doi: 10.1016/j.cose.2024.103938.
[15] E. C. K. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, Art. 192, 2022, doi: 10.3390/info13040192.
[16] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, Art. 39, 2021, doi: 10.3390/fi13020039.
[17] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. Breitner, "Information security awareness and behavior: A theory-based literature review," *Manag. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, 2014, doi: 10.1108/MRR-04-2013-0085.
[18] P. Kautwima, V. Hashiyana, and T. Haiduwa, "Information security mechanisms and ICT policy in practice: A case of the University of Namibia," *Int. J. Wireless Commun. Mobile Comput.*, vol. 9, no. 2, pp. 7–15, 2021, doi: 10.11648/j.wcmc.20210902.11.
[19] N. S. Fouad, "Securing higher education against cyberthreats: From an institutional risk to a national policy challenge," *J. Cyber Policy*, vol. 6, no. 2, pp. 137–154, 2021, doi: 10.1080/23738871.2021.1973526.
[20] I. S. Bianchi, R. D. Sousa, and R. Pereira, "Information technology governance for higher education institutions: A multi-country study," *Informatics*, vol. 8, no. 2, Art. 26, 2021, doi: 10.3390/informatics8020026.
[21] EDUCAUSE, "Cybersecurity governance toolkit," *EDUCAUSE Rev.*, Jan. 2024. [Online]. Available: https://er.educause.edu/articles/2024/1/cybersecurity-governance-toolkit
[22] J. Prümmer, "A systematic review of current cybersecurity training methods," *Comput. Secur.*, vol. 125, Art. 103585, 2024, doi: 10.1016/j.cose.2023.103585.
[23] S. Trang and B. Brendel, "A meta-analysis of deterrence theory in information security policy compliance research," *Inf. Syst. Front.*, vol. 21, no. 6, pp. 1265–1284, 2019, doi: 10.1007/s10796-019-09956-4.
[24] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: A higher education case study," *Inf. Comput. Secur.*, vol. 26, pp. 91–108, 2018, doi: 10.1108/ICS-09-2016-0073.
[25] G. N. Angafor, "Game-based learning: A review of tabletop exercises for cybersecurity incident response training," *Secur. Privacy*, vol. 3, no. 5, Art. e126, 2020, doi: 10.1002/spy2.126.
[26] C. M. Patterson *et al.*, "Learning from cyber security incidents: A systematic review," *Comput. Secur.*, vol. 124, Art. 103309, 2023, doi: 10.1016/j.cose.2023.103309.