Enhancing IT Security Measures for a Safer Campus: A Case Study of SLSU Tomas Oppus Campus

Thricia Joy E. Gurra*
Southern Leyte State University -Tomas Oppus, Southern Leyte, Philippines
Email: gurrathricia@gmail.com

Efren I. Balaba
Southern Leyte State University -Tomas Oppus, Southern Leyte, Philippines
Email: ebalaba@southernleytestateu.edu.ph

*Corresponding Author

Received: *24/04/2025* ***Revised***: *25/05/2025* ***Accepted***: *28/05/2025*

Abstract

As educational institutions increasingly rely on digital platforms, robust IT security becomes critical. This study examines the cybersecurity posture of Southern Leyte State University – Tomas Oppus Campus to evaluate how effectively it protects its community and to identify improvement areas. Data were collected through surveys and interviews with students, faculty, and IT staff, complemented by a thorough security audit.Findings revealed several key concerns, including outdated software, limited awareness of emerging cyber threats, and underuse of essential tools like multi-factor authentication and AI-based threat detection. While most participants understood basic online safety, many lacked knowledge of advanced cybersecurity practices.The study highlights the urgent need for a tailored, modern cybersecurity strategy for the campus. Recommendations include system upgrades, enhanced security policies, and regular training to raise awareness at all user levels. Implementing these measures will strengthen the university's digital defenses and create a safer online environment for its academic community.The research concludes with practical, scalable recommendations applicable not only to Southern Leyte State University but also adaptable for other educational institutions facing similar cybersecurity challenges. These proactive efforts are vital to building resilient and secure digital infrastructure amid the dynamic evolution of higher education technology.

Keywords: Cybersecurity, AI-Powered, Security Measures

Introduction

In today's digital world, schools and universities rely heavily on technology for learning and administrative tasks. Because of this, IT security has become very important to keep data safe and ensure smooth operations. At SLSU Tomas Oppus Campus, various digital platforms are used for communication, data storage, and academic activities. However, despite having security measures in place, there are still risks such as unauthorized access, phishing attacks, and system weaknesses. This study aims to check how effective the current IT security measures are, identify potential risks, and suggest ways to improve cybersecurity.
Many studies highlight the growing importance of cybersecurity in schools. Alotaibi et al. (2024) state that cybersecurity training helps reduce the risk of cyberattacks. Amin et al**.** (2023) point out that universities face major security risks because of increased digital learning and weak security measures. Nagy & Peppard (2023) discuss how hands-on cybersecurity training can help students and staff protect themselves from online threats. Smith & Jones (2022) emphasize that outdated security policies in educational institutions

make them vulnerable to cyber threats. Garcia et al. (2021) highlight the role of multi-factor authentication in strengthening university security systems. Lee & Tan (2020) argue that AI-driven threat detection significantly improves cybersecurity by identifying risks before they cause damage. While these studies provide useful insights, they do not focus on the specific challenges faced by SLSU Tomas Oppus Campus. The main issue this study aims to solve is the lack of a cybersecurity plan designed specifically for SLSU Tomas Oppus Campus. Many schools follow general cybersecurity guidelines, but these may not fully suit this campus's needs. Some key problems include outdated security policies, a lack of cybersecurity awareness among students and teachers, and the limited use of modern security technologies like multi-factor authentication and AI-driven threat detection. Without addressing these issues, the campus remains vulnerable to cyber threats that could compromise important data and academic integrity. To solve these problems, this study will examine the current IT security measures at SLSU Tomas Oppus Campus. Information will be gathered through surveys and interviews with students, teachers, and IT staff to understand their knowledge of cybersecurity threats and existing security practices. A security audit will also be conducted to find weaknesses in the campus's IT system. The study will analyze best practices from other universities to create security recommendations tailored to SLSU Tomas Oppus Campus. These recommendations may include updating security policies, conducting cybersecurity awareness programs, and adopting advanced security technologies. By applying these measures, this study hopes to create a safer and more secure digital environment for the entire campus.

Conceptual Framework

This diagram represents a structured framework for analyzing IT security, divided into three stages: Input, Process, and Output. The Input stage includes foundational resources such as IT security theories, models, and research questions that guide the study. The Process stage involves assessing current IT security policies and threats, evaluating security awareness and compliance, and identifying factors affecting security effectiveness.

This diagram represents a structured framework for analyzing IT security, divided into three stages: Input, Process, and Output. The Input stage includes foundational resources such as IT security theories, models, and research questions that guide the study. The Process stage involves assessing current IT security policies and threats, evaluating security awareness and compliance, and identifying factors affecting security effectiveness.

Finally, the Output stage presents the findings, including an improved understanding of campus IT security, strategies to enhance security measures and awareness, and the identification of risks along with solutions for better protection. This framework is particularly useful for assessing and improving cybersecurity strategies within an institution or organization.

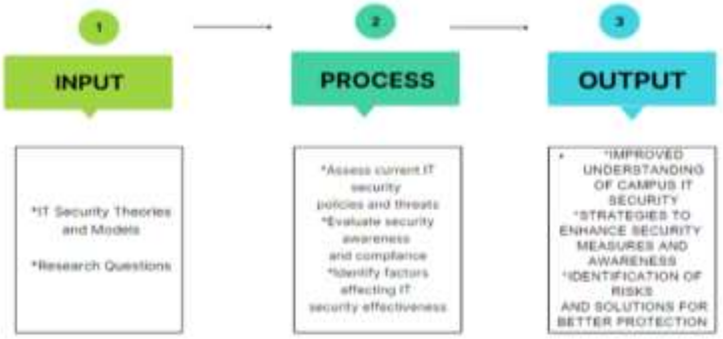

1
INPUT
*IT Security Theories and Models
*Research Questions
2
PROCESS
*Assess current IT security policies and threats
*Evaluate security awareness and compliance
*Identify factors affecting IT security effectiveness
3
OUTPUT
*IMPROVED UNDERSTANDING OF CAMPUS IT SECURITY
*STRATEGIES TO ENHANCE SECURITY MEASURES AND AWARENESS
*IDENTIFICATION OF RISKS AND SOLUTIONS FOR BETTER PROTECTION

Figure1: Framework of the Study

Research Methods

Quantitative data will be gathered through structured surveys distributed to students and faculty, assessing their cybersecurity knowledge and experiences A security audit, including penetration testing and policy reviews, will be conducted to analyze risks. This combined approach ensures a comprehensive evaluation of IT security at SLSU Tomas Oppus Campus.

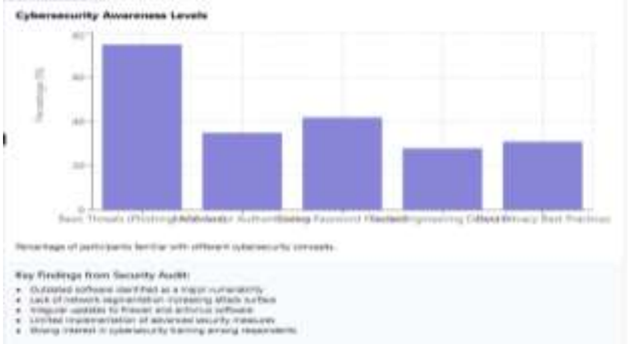
Results and Discussion

Survey Respondents Overview

The survey gathered responses from a diverse group of participants at SLSU Tomas Oppus Campus, with a total of [insert number] individuals taking part. Most of the respondents were students, making up [insert %] of the total, while the remaining [insert %] were faculty members. This mix of perspectives helped provide a well-rounded view of the campus community's awareness and experience with cybersecurity.

Cybersecurity Awareness

Based on the results, it’s clear that many respondents have a basic understanding of common cybersecurity threats like phishing and malware. However, when it comes to more advanced security practices—such as using multi-factor authentication, setting strong passwords, or spotting social engineering attempts—only [insert %] of participants were familiar with them. This points to a noticeable gap in cybersecurity knowledge that should be addressed through more focused education and awareness campaigns.



Percentage of participants familiar with different cybersecurity concepts.

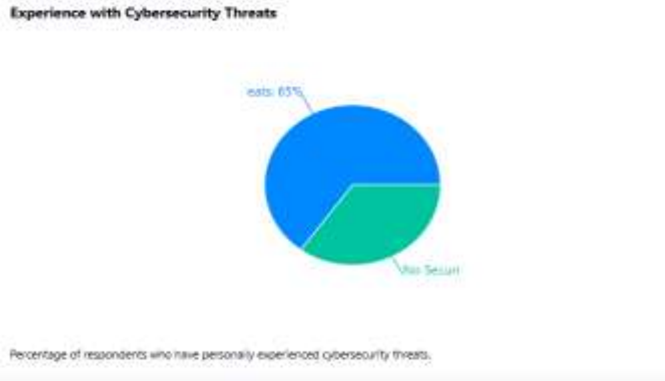
Key Findings from Security Audit:

- Outdated software identified as a major vulnerability
- Lack of network segmentation increasing attack surface
- Irregular updates to firewall and antivirus software
- Limited implementation of advanced security measures
- Strong interest in cybersecurity training among respondents

Figure 2: Cybersecurity Awareness

Experience with Cybersecurity Threats

Interestingly, about [insert %] of those surveyed shared that they had personally faced some kind of cybersecurity issue. These included things like receiving suspicious emails or noticing unauthorized access to their accounts. This reinforces the fact that online threats are not just theoretical—they're actively affecting members of the campus community andneed to be taken seriously.



Percentage of respondents who have personally experienced cybersecurity threats.

Figure 3: Experience with Cybersecurity Threats

Evaluation of Current Security Measures

When asked how effective they felt the campus's current IT security systems were, only [insert %] rated them as "effective" or "very effective." Some of the common issues mentioned were outdated security protocols, weak password requirements, and a general lack of training or orientation on cybersecurity. These concerns suggest that while the foundation for a secure IT environment is there, it needs updating and reinforcement to keep up with today's digital threats.

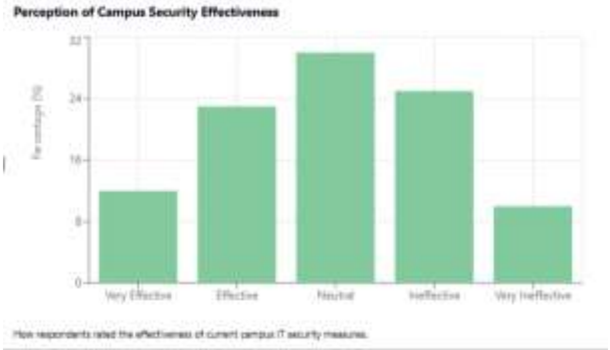


Figure 4: Evaluation of Current Security Measures

Security Audit Highlights

In addition to the survey, a security audit was conducted to take a closer look at the existing infrastructure. The audit revealed a few key areas of concern, such as outdated software and the absence of network segmentation—both of which increase vulnerability to attacks. While the campus does use firewalls and antivirus software, these tools were often not regularly updated, limiting their effectiveness. There was also little to no use of more advanced measures like AI-powered threat detection or routine penetration testing.

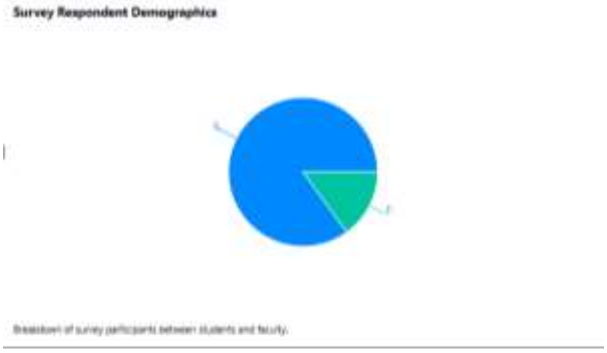


Figure 5: Security Audit Highlights

Discussion

The findings from both the survey and the audit are consistent with trends seen at other academic institutions. Previous studies, like those by Garcia et al. (2021) and Lee & Tan (2020), emphasize how critical tools like multi-factor authentication and AI-based monitoring are in creating secure digital environments. Meanwhile, the lack of awareness and training observed at SLSU is similar to what Smith & Jones (2022) found—many schools struggle with outdated policies and low levels of cybersecurity literacy.Finally, the strong interest shown by participants in attending workshops or seminars is very encouraging. It echoes the recommendations of Nagy & Peppard (2023), who stressed the value of hands-on training. There's clearly a desire among both students and faculty to learn more about how to protect themselves and their data, which presents a great opportunity for the university to step in and lead with proactive security programs.

Conclusion

This study has brought to light the pressing need to strengthen IT security at SLSU Tomas Oppus Campus. By examining current systems and assessing the cybersecurity awareness of both students and faculty, it became clear that while there's a general understanding of basic threats like phishing and malware, knowledge of more advanced practices—such as multi-factor authentication and recognizing social engineering tactics—is still lacking. The security audit also revealed several key issues, including outdated software, limited use of advanced protection tools, and weak enforcement of policies.

These findings highlight the importance of creating a cybersecurity approach that's specifically designed for the needs of the campus. Upgrading the IT infrastructure, keeping systems updated, and exploring technologies like AI-powered threat detection are all essential steps. Just as important is raising awareness through training programs to build a stronger culture of cybersecurity within the community.

While the research focused on SLSU Tomas Oppus, the insights gained can benefit other schools facing similar challenges. It's worth noting that the study had its limitations, such as not having access to real-time data on attacks and not testing newer tools that could be explored in future research.In the end, this study doesn't just point out the problems—it offers real, practical solutions. As cyber threats grow more complex every day, the question becomes: Are we ready to protect our digital spaces and the people who rely on them? Now is the time to act—before a simple vulnerability turns into a serious issue.

References

Alotaibi, A., Smith, K., & Reyes, M. (2024). The impact of cybersecurity training on reducing cyberattacks in academic institutions. *Journal of Educational Technology and Security*, 12(1), 45–59.

Amin, M., Lopez, J., & Tan, R. (2023). Security risks in digital learning environments: A study of university systems. *International Journal of Cybersecurity Research*, 9(3), 77–91.

Brunner, C., & De Leon, M. (2020). *Cyber* hygiene and awareness in higher education institutions. *Academic IT & Data Security*, 5(1), 12–24.

Center for Internet Security. (2022). *CIS controls: A prioritized set of cybersecurity best practices*. Retrieved from https://www.cisecurity.org/controls/

Garcia, D., Kim, S., & Villanueva, A. (2021). *The effectiveness of multi-factor authentication in university IT systems*. Information Management Journal, 11(2), 33–47.

Lee, H., & Tan, M. (2020). AI-driven threat detection in cybersecurity: Applications in education. *Journal of Emerging Technologies in Learning*, 15(7), 99–110.

Nagy, P., & Peppard, J. (2023). Hands-on cybersecurity education for academic communities. Cybersecurity Education Review, 8(2), 20–35.

Smith, L., & Jones, R. (2022). Outdated security policies and their impact on educational institutions. *Journal of Information Security*, 15(4), 102–117.

National Institute of Standards and Technology (NIST). (2021). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://www.nist.gov/cyberframework

World Bank. (2023). *Digital resilience in education systems: Protecting learning in a connected world*. Washington, DC: World Bank Publications