SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 11 | November 2024 - Peer Reviewed Journal

# CHALLENGES IN SAFEGUARDING THE CYBERSECURITY MEASURES AMONG HIGHER EDUCATION INSTITUTIONS IN THE NATIONAL CAPITAL REGION

**Kier Gabriel E. Tampos**
*The Faculty of the Graduate School Philippine, College of Criminology, Philippines*

**ABSTRACT**
*Higher Education Institutions are using various Management Information Systems as their main repository of the vast data that schools acquire from their stakeholders. On this dependency on technology the paradox of its misuse of platforms entailed breach on sensitive information, operational protocols, and even communication. Hence, creating a much demand for its heightened focus on safeguarding the institution's digital environments, through dynamic security measures and creating a much more technologically advanced landscape. As the call for safeguarding the digital environment, among Higher Education Institutions have resulted in strengthening their protection, however, even how much commercially offered software and systems are made available cyberthreats are still common to the said industry. Hence, the study purports to see the challenges in safeguarding the cybersecurity measurements being implemented by the HEIs in the National Capital Region that may stop or prevent cyberthreats and attacks as well as checking on the resiliency and awareness of its employees as they are the first line of defense. Using a descriptive-correlational approach, the data serves as the anchor-points of the proposed countermeasures that the cybersecurity framework has to offer.*

**KEYWORDS:** *Cybersecurity, Cyberthreat, Cyber Attack, Higher Education Institutions, National Capital Region*

## INTRODUCTION

In the contemporary landscape of Higher Education Institutions throughout the world, the effective functioning of Management Information Systems (MIS) as a repository of vast data is integral to their operations. The reliance on digital platforms for managing sensitive information, operational processes, and communication demands a heightened focus on safeguarding their digital environments with the security measures they implement in a dynamic and technologically advanced landscape. Connections with other institutions internationally opened the issues on the protection of critical data, confidentiality of client information, and the overall integrity of their information systems which has become the paramount consideration in the age of artificial intelligence.

In the event that cybersecurity is critical, global collaboration becomes essential for effective incident response. Since academic institutions are centers of learning, knowledge and generation of noble information, cybersecurity measures developed by the employees of schools are highly responsive to cybersecurity issues and cyberattacks, but only for the meantime. This is because of the dynamic and evolving landscape of cyberspace. Globalization aids in the creation of protocols in coordinating with relevant authorities across borders to mitigate the impact of cybersecurity breach and cyberattacks that target sensitive information, including personal data as part of their operations. As such, international data protection laws have been forged to mitigate the effects of cyberattacks, such as the European Union's General Data Protection Regulation (GDPR).

The academic landscape is a complex structure where some key aspects, challenges and problems related to cybersecurity in the context of higher education on the international level need sustainability and resiliency. The promotion of cybersecurity awareness remains inadequate since the incidents are mostly linked with human error. The problems encountered by schools throughout the world are not uniform since they vary as to the degree or gravity, frequency and effects. There are no uniform security measures implemented globally because of jurisdictional concerns and legal compliance in each political unit. On a wider perspective, it is considered as an advantage for cybercriminals when different countries do not treat the acts leading to cybercrimes similarly.

### International Background

The worldwide panorama of protecting the digital environments with cybersecurity measures implemented by Higher Education Institutions with their Management Information Systems (MIS) is defined by the intricate interactions between global cybersecurity threats, legal frameworks, and technology developments. Just like any other organization holding a great volume of information or data,

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 11 | November 2024 - Peer Reviewed Journal

HEIs are subject to a wide range of cyberthreats that cut across national borders since they operate internationally.
The nature of cyber threats is transnational and continually evolving along with the dynamics of the society. Threat actors, including state-sponsored entities, cybercriminal organizations, and hacktivists, operate on a global scale. Safeguarding digital environments with security measures must therefore address a broad spectrum of potential threats. Various international standards and frameworks provide guidance for cybersecurity best practices such as, but not limited to the ISO/IEC 27001 for information security management and NIST Cybersecurity Framework. HEIs may adopt these standards to enhance their digital security posture and demonstrate compliance on a global scale.

The international landscape of safeguarding digital environments of schools in their Management Information Systems (MIS) is characterized by a complex interplay of global cybersecurity challenges, regulatory frameworks, and technological advancements. As Higher Education Institutions (HEIs) operate across borders and engage in cross-jurisdictional activities due to their foreign linkages, they are exposed to a myriad of cyber threats that transcend national boundaries. Understanding the international background of safeguarding digital environments is crucial for these agencies to effectively navigate the evolving landscape of cybersecurity.

**National Background**
In the Philippines, safeguarding digital environments within the Management Information Systems (MIS) of HEIs is of utmost importance since these are centers of learning, honing of knowledge and skills and centers for research and development that are vital in societal development. The amount of data they possess may be useful for cybercriminals in perpetrating cyber offenses, such as scamming, phishing and remote or online access to an individual's accounts. Although much emphasis is given to business organizations, financial institutions or banks in particular due to the monetary gains of cybercriminals, academic institutions also suffer the impacts of cyberattacks and breach to their digital environment security, whether monetary or not. The country's dynamic cybersecurity landscape, regulatory framework, and technological advancements shape the approach to securing the digital assets of every institution or organization.

On the national cybersecurity policy, the Philippines had been actively working on enhancing its national cybersecurity policies, in which institutions or organizations are expected to align their digital security measures or practices with the country's cybersecurity frameworks and guidelines issued by government agencies, like the Department of Information and Communications Technology (DICT). The Data Privacy Act of 2012 (Republic Act No. 10173) imposes obligations towards organizations that handle personal information. Hence, HEIs must comply with the said law by implementing data protection measures, and secure the confidentiality of client and employee data stored in their MIS. Despite the severity of the penalty, cybersecurity issues remain active and even reached its height during the pandemic

The National Privacy Commission is the regulatory body responsible for enforcing the Data Privacy Act including NPC regulations, advisories, and guidelines that may impact the digital security practices of HEIs and other institutions. Government-led initiatives and partnerships aimed at enhancing national cybersecurity where every organization must actively participate.

Collaborative efforts with government agencies can include information sharing, capacity-building programs, and joint cybersecurity exercises that may be useful to every HEIs security measures.

**Local Background**
The security landscape of Higher Education Institutions (HEIs) in the NCR, are oftentimes infiltrated with cyber-attacks and maligned with the poor firewall, security measures implemented or cybersecurity in the academe. This often invites hackers preying on the weak cyber defenses of institutions which were established by poor, incompetent and fly-by-night security providers, still in the trial stage, or free services with less security features. As a result, the integrity of the data being handled and secured by the institution ends up infiltrated and used for other unauthorized and illegal purposes. This is the very threat in the digital environment.

Cybersecurity implemented in different HEIs are all effective, as long as they are properly maintained by employees with full knowledge of security awareness and best practices combating cyberthreats. Measuring the level of effectiveness of cybersecurity is subjective to the HEIs, depending on various circumstances, such as the amount of data stored in their MIS, the operating capacity of the institution and the prevalence of online transactions as a business practice adopted. The dynamic and evolving landscape of cybersecurity shifts the effectiveness of cybersecurity measures.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 11 | November 2024 - Peer Reviewed Journal

Since there is no guarantee when cyberattacks occur, HEIs must be ready at any time to patch any vulnerability that they notice, before hackers take advantage of the weakness in the security measures. Any form of breach in the security measures exposes the held data to cyberattacks, and the said data may be used to perpetrate any form of cybercrime where hackers may greatly benefit. Problems of some institutions to come up with a strong cybersecurity are linked with their available resources and financial capability. At the end, their cybersecurity implemented is weak and vulnerable to cyberattacks. Others also end up with outdated software and vulnerable legacy systems.

The implementation of cybersecurity measures by the HEIs to protect their data necessitates the capacitation of their employees on cybersecurity awareness and adherence to security policies that are critical. Problems are encountered by HEIs in implementing their cybersecurity when limited personnel or less-qualified employees are hired to monitor the cybersecurity performance. This is the main reason why problems are encountered at the implementation stage, and such problems are mitigated when employees are capacitated in cybersecurity issues. Vulnerabilities and weaknesses can be detected and addressed by qualified employees before hackers exploit them through an effective intrusion detection and prevention system. Solutions or countermeasures to the encountered problems come with the cybersecurity resilience framework or model.

## METHODOLOGY

### Research Design

This study used a descriptive-correlational research design utilizing quantitative data under the quantitative research methods. Through the research design used, the research investigations seek to demonstrate the link between several variables and give statistical representations. The design was suitable as the researcher gathered information relevant to a participant's behavior or attitude in order to perform the assessments needed in the study.

The variables were measured as they happen, such as the profile of the Higher Education Institutions (HEIs) in terms of years of operation (year established up to present), current number of employees, capability for online transactions, average number of students in the last five years, existing number of linkages with local/national institutions (academic, non-academic, community-based, NGOs, and the like), existing number of linkages with foreign institutions (academic, non-academic, community-based, NGOs, and the like), digitized records system and types of cybersecurity measures implemented; effectiveness of the cybersecurity measures implemented in terms of cybersecurity structure, anti-virus and anti-malware software, data encryption, access controls, security structure, and network monitoring tool; level of awareness of the employees of the Higher Education Institutions (HEIs) on cybersecurity in terms of the types of cybersecurity or domains, common cybersecurity threats, common and dangerous cybersecurity myths, key cybersecurity technologies and best practices, Management Information System, and related solutions; and challenges encountered in implementing the cybersecurity measures.

The results of the evaluation of the effectiveness of security measures implemented, awareness of the respondents on cybersecurity and challenges encountered were correlated with the profile of the HEIs. Likewise, the profiles were also used as predictors of effectiveness, awareness and challenges encountered in the implementation of cybersecurity measures. The results were used as the basis of a proposed Resilient Cybersecurity Model, a framework of enhanced cybersecurity measures for HEIs use.

### Research Method

This study utilized quantitative research through survey methods or use of a researcher-made questionnaire. Research methods refer to the systematic approaches and techniques employed to gather, analyze, interpret, and draw conclusions from data in a structured and rigorous manner. The researcher adequately constructed a survey questionnaire-checklist sufficient to gather the needed data to complete the study.

Through survey technique, the researcher used the research instrument that was validated by experts and later on assessed with reliability statistics to assure the internal consistency of the items. Once reliable, the data were gathered through the research instrument that was floated or sent to the respondents both via online or through Google Forms and face-to-face administration of the instrument after the researcher made appointments to the qualified respondent in each HEI of NCR. The final data were simplified in a matrix for systematic data analysis using the appropriate statistical tools, and facilitated by the use of IBM SPSS v.29 software as to the computations.

### Population of the Study

The respondents of this study were the representatives from different Higher Education Institutions (HEIs) of the National Capital Region (NCR). Each HEI included in this study was represented by one (1) employee whose qualifications must conform to the order identified by the researcher: must be the head, director, supervisor, a key employee, or any authorized representative of the HEI's

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 11 | November 2024 - Peer Reviewed Journal

Management Information System (MIS) or equivalent office. In the absence of MIS, the dean, program chair/head of the College of Information Technology or Studies, Computer Science, Computer Management, Computer Engineering, or any professor or instructor in the same field, or any authorized employee by the HEI.

**Locale of the Study**

The research focused on the Higher Education Institutions (HEIs) operating in the National Capital Region, based on the list of recognized HEIs by the Commission on Higher Education (CHED). With the dynamic landscape of educational technology, HEIs throughout the country have leveled up their online environment in response to progress and globalization. All academic institutions have been forced to innovate and embrace technology in education since the pandemic in 2020. Those who failed to embrace technology were forced to close and shut down their operations.

**Scope and Limitation of the Study**

This study was emphasized on the results of the evaluation of the security measures implemented by selected Higher Education Institutions (HEIs) within the National Capital Region as means to protect their possessed digital and online information, ensure confidentiality and integrity of data in their respective Management Information System (MIS). The results were the basis of the proposed Resilient Cybersecurity Model, a framework of enhanced cybersecurity measures for the HEIs.

The independent variables used were the profile of the HEIs and their existing or implemented cybersecurity measures. The dependent variables were the assessment or evaluation of the cybersecurity measures of the HEIs as to the effectiveness of the cybersecurity measures, awareness of the employees of HEIs on cybersecurity, and challenges encountered in implementing their own cybersecurity measures. Correlation and regression analysis revealed the predictors and the cause-and-effect relationship of variables.

Limitations include the level and status of implementation of cybersecurity measures in different HEIs relative to their financial resources, revenues derived in their operations, facilities, equipment, physical structures, and online capabilities. The results of the assessment or evaluation may be subjective for each HEI as to the effectiveness of their cybersecurity measures being implemented. The challenges encountered in each HEI may be viewed differently by other HEIs depending on their capabilities. Further, the size of the HEIs (number of students), facilities for online transactions, engagement and utilization of the Internet, online capabilities and technological inclination also set limitations to this study since there is no minimum requirement or standard for HEIs in their online or technology usage.

On the part of the researcher, limitations existed as regards the time and situation when the instrument was administered or floated, and the availability of the respondents that was far more challenging than the gathering of data.

**Data Gathering Tool/s**

The researcher used a self-constructed or researcher-made research instrument in gathering the data. The instrument was divided into four parts. The first part inquired on the profile of the respondents that the statement of the problem provided, and a checklist was designed by the researcher to facilitate accurate response from the participants. Other information or data about the HEIs were also accessible in their official website. The second part measured the effectiveness of the cybersecurity measures of the HEIs implemented in the digital environment of their MIS in terms of cybersecurity structure, anti-virus and anti-malware software, data encryption, access controls, security structure and network monitoring tool. The third part measured the awareness of the employees of HEIs on cybersecurity in terms of types of cybersecurity or domains, common cybersecurity threats, common and dangerous cybersecurity myths, key cybersecurity technologies and best practices, Management Information System (MIS) and related solutions. The fourth part assessed the challenges encountered in the implementation of cybersecurity measures by

Higher Education Institutions (HEIs).

The research instrument was crafted and conceptualized by the researcher based on the information provided at the IBM website, literature review and existing studies, law, policies and other pertinent sources with legal implications. Although self-constructed, the instrument contained guided and carefully chosen information that satisfied the criteria and contents needed for the study. Chapter 2 contained the related literature and studies used by the researcher as a springboard to complete the research instrument.

The instrument or tool of this research was subject to different scrutiny. The initial draft of the researcher was checked and edited by an external consultant of research as preparatory in the initial draft. When finalized, the researcher sent the instrument to three experts for purposes of validation by experts in the field of cybersecurity, academe and practitioners in the information and communications technology. The assessment of validity were based on the Face Validity which proved that the items in the measurement or instrument

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 11 | November 2024 - Peer Reviewed Journal

linguistically and analytically look like what was supposed to be measured based on the assessment in each item by the selected experts or validators; Content Validity which ensured that the items of the instrument were relevant and representative of the target construct using the Content Validity Ratio (CVR) or Lawshe's Method, where the CVR depends on the number of validators who assessed the instrument; and the Criterion-based Validity which ensured that the outcomes of the study were measured by the items of the instrument. Their certification and validation assessments were appended for reference purposes.

**Data Gathering Procedure**

The procedure in data gathering commenced from the time the research instrument was fully assessed of its validity and reliability. From thereon onwards, the researcher sent communication letters or notices, both printed in black and white and email to all the 328 HEIs of NCR, since others might not participate in the study. The HEIs that gave their consent on the study, or replied with the communication sent to them were either sent with a questionnaire in Google forms, or visited by the researcher for personal administration of the research instrument. Hence, the survey instrument was floated or administered to the respondents both in person and through online means.

To ensure the integrity of the data, the researcher ensured that before the respondents answered the questionnaire, they understood the purpose and objectives of the study. Further, the consent of the respondents was given freely before they began answering. Ample time was given to the respondents in completing their responses. Once done, the researcher retrieved the instrument personally, and for the online responses, the respondents must submit the completed survey forms to complete the process, and the data were extracted by the researcher from the Google documents.

The complete data of the study were simplified in a matrix, where all the data from the sample respondents need to be placed. Incomplete data or responses coming from any respondent were disregarded since they affected the integrity of the whole study or the missing data were substantial. The responses made through online means were gathered by downloading the responses and extracting them carefully to be included in the paper-based results, in the matrix earlier prepared to maintain the integrity and accuracy of the data. The researcher gathered the data from the respondents within a 25-day period. Thereafter, the simplified data were exported to the IBM SPSS v.29 software for treatment, computations and analysis that aided the researcher in interpreting the results and made inferences.

**Treatment of the Data**

The following statistical tools were used in the analysis of data and interpretation of the results:

**Frequency Count and Percentage** is used in the descriptive measurement of data in the profile of the respondents such as education, eligibility, appointment; position, years in industry and seminar attended.

**Pearson Product Moment of Correlation (Pearson r)** was used in determining the significant relationship between interval or ratio data or variables such as the profile of HEIs (years of operation, number of employees, average number of students in the last five years, existing number of linkages with local/national institutions and existing number of linkages with foreign institutions) and the effectiveness of cybersecurity measures implemented and awareness of the employees on cybersecurity.

## RESULTS AND DISCUSSION

**It can be gleaned below the summary of findings of the research:**

*Most of the respondents came from private schools/universities and most of the schools existed for more than 20 years in* ***terms of operations****. For the* **Current Number of Local Employees,** *most of the HEIs have 201-300 employees.* **On the Average Number of Students for the last five years,** *majority of the HEIs had 15,001-20,000 students in the last five years.* **For Capability for Online Transactions,** *majority of the HEIs are capable in online transactions.* **For Digitized Records System,** *majority of the HEIs are digitized in records system.* **In line with the Number of Existing Linkages with Local/National Institutions,** *all HEIs have local linkages* **same with the Number of Existing Linkages with Foreign Institutions,** *all HEIs have foreign linkages.*

The HEIs have all of the types of cybersecurity measures implemented when it comes to **Types of Cybersecurity Measures Implemented and** *all of the HEIs have a stiff cybersecurity measures.*

**On the Effectiveness of Cybersecurity Measures Implemented,** *it can be concluded that most of the respondents strongly agreed on the imposed cyber security of the HEIs while* **On the Effectiveness of Cybersecurity Measures Implemented (Anti-Virus and Anti-Malware Software) ,** *the HEIs the anti-virus and anti-malware software of the HEIs protect the institutions.*

**On the Effectiveness of Cybersecurity Measures Implemented (Data Encryption)** *the HEIs have a safe and sound standards of security with regards to data encryption.* **On the Effectiveness of Cybersecurity Measures Implemented (Access Controls**

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 11 | November 2024 - Peer Reviewed Journal

**Indicators) ,** *the HEIs' portals and data can be accessed only by the authorized stakeholders of the HEIs.* **On the Effectiveness of Cybersecurity Measures Implemented(Security Structure Indicators),** *there is a need for thorough information dissemination to the employees of the HEIs in line with the cybersecurity structure of the HEIs.* **On the Effectiveness of Cybersecurity Measures Implemented (Network Monitoring Tool Indicators),** *there is a need for thorough information dissemination to the employees of the HEIs in line with the cybersecurity structure of the HEIs.*

**On the Awareness of HEI Employees on Cybersecurity (Types of Cybersecurity or Domains Indicators),** *the employees of the HEIs are aware of the cybersecurity measures of their respective institution.* **On the Awareness of HEI Employees on Cybersecurity (Common Cybersecurity Threats indicators Indicators),** *the employees of the HEIs are aware of the effects on the services and operations of the HEIs once a glitch in the system will take place.* **On the Awareness of HEI Employees on Cybersecurity (Myths or Misconceptions Indicators),** *the employees of the HEIs are aware of the effects on the services and operations of the HEIs once a glitch in the system will take place.*

**On the Awareness of HEI Employees on Cybersecurity (Key Cybersecurity Technologies & Best Practices),** *the employees of the HEIs are somewhat agreed on the awareness about the daily monitoring of the glitches in the HEIs.*

**On the Awareness of HEI Employees on Cybersecurity Management Information System (MIS) Indicators,** *the employees of HEIs are strongly agreed on the awareness regarding the existence and functions of the MIS.*

**On the Awareness of HEI Employees on Cybersecurity Related Solutions indicators ,** *HEIs employees had somewhat agreed on the features of the cybersecurity of their company/institutions.*

**On the Challenges Encountered in Cybersecurity Implementation,** *the HEIs have ways and means to address the challenges of the cybersecurity implementation.*