

## Cybersecurity program for Philippine higher education institutions: A multiple-case study

Noly M. De Ramos<sup>1</sup>, Francisco Dente Esponilla II<sup>2</sup>

<sup>1</sup>Faculty of Technology and Livelihood Education, Philippine Normal University, Ermita, Philippines

<sup>2</sup>University Research and Development Services, Technological University of the Philippines, Ermita, Philippines

---

### Article Info

#### Article history:

Received Sep 5, 2021

Revised May 26, 2022

Accepted Jul 1, 2022

---

#### Keywords:

Academic integrity

Cybercrime

Cybersecurity

Internet of things

Program logic model

---

### ABSTRACT

Digital technology has become an integral aspect of an educational system. Every state university funded the creation of Information Technology Offices to secure its Management Information System. The challenge on cybersecurity threatens the intellectual capital of students especially in a research university, theft of crucial information, and financial loss. The current study is a multiple case study of cybersecurity threats and challenges of Selected Philippine State Universities and Colleges in the National Capital Region. Sample participants were purposively selected Information Technology experts from various selected State College and Universities. A structured interview as the main instrument of the study investigated threats and challenges of cybersecurity to assess active and proactive approaches to developing a model framework for security resources in respective academic institutions. Responses gathered from the interview were consolidated and analyzed through a thematic coding process. The result of the study revealed the following challenges in cybersecurity are user education, cloud security, information security strategy, and unsecured personal devices. The creation of a program logic model will provide an informed cybersecurity planning, implementation, and assessment framework to the commission on higher education in collaboration with the Department of Information and Communication Technology, and the Philippine Association of the State Colleges and Universities.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

### Corresponding Author:

Francisco Dente Esponilla II

University Research and Development, Technological University of the Philippines

Ayala Boulevard, Ermita, Metro Manila 1000, Philippines

Email: francisco\_esponilla@tup.edu.ph

---

## 1. INTRODUCTION

Cybersecurity is a constitutional issue that comprises different political players like government agencies, academic institutions, and private organizations. However, cybersecurity might affect the political practices and collaboration among nations, regions, international organizations, and private institutions [1]. This would result in differences in the implementation rules and regulations, policies, and frameworks. Moreover, developing cumulative cybersecurity is challenging due to the reasons that “cybersecurity is largely covered with privacy, over-classification, and the customary main stakeholders are in the field of national defense and intelligence agencies [2].

Cybercrime Prevention Act of 2012 under Republic Act 10175 [3] was signed into law, finally, the Supreme Court of the Philippines (SC) has finally placed down the rules of court in the issuance of warrants and related orders in the enforcement of punishable acts as provided in the law. It is being noted that the rule supplements the Rules of Criminal Procedure on the preliminary investigation where all points prosecution of

criminal action and all crimes enumerated involving violations of RA 10175 in the said with the use of information and communications technologies (ICT) are cognizable by the Regional Trial Courts (RTCs) in the country and those courts specifically designated as “cybercrime courts.”

There is already available technical expertise that implements proportionate controls to different parts of systems and networks in state universities and colleges (SUC) [4]. However, there are no definitive roles and responsibilities to effective cybersecurity that extends across the institution [5]. A precise challenge for SUCs is to develop appraised lawful assessment, financial and reputational conveyed by the various available information they have. Institutions must ruminate and develop models of risk management and assessment that are associated with research data management, policies, and practices. Venter *et al.* [6] suggested that measures should determine proportionate and appropriate controls that focus on protecting vulnerable information while supporting the research, the teaching and learning culture that is basic institutional concerns.

The National Cybersecurity Plan 2022 [7] cited that during the Arroyo administration in 2004 emphasized the establishment of National Cybersecurity Plan is rolled out as one of the bases for crafting the proposed information security incident response manual through the ICT office and now the newly formed Department of Information and Communications Technology. In 2015, Executive Order No. 189 created the National Cybersecurity Inter-Agency (NCIA) was signed. This very important event leads to the necessary undertaking insightful of the Philippines Vision towards a safe Philippine Cyberspace. The purpose of this endeavor is to build one direction and coordination between government agencies and other relevant sectors to collaborate in developing an agreement that addresses national response, and direct assessment and actions in preparation of appropriate and effective measures to support cybersecurity capabilities against current and future cyber threats.

Cybersecurity problem exists despite of the researchers’ recommendations of the necessity of cybersecurity protection and the availability of governmental measures, the prevalence of hacking and information threats are at stake. In this era of the Internet of Things (IoT), and the COVID-19 pandemic dictates online activities of all economic players such as the academic community, the industry, and other government-owned and private agencies. Hence, the purpose of this study is to explore cybersecurity challenges, and measures as input to the program logic model (PLM) that could aid the crafting of the updated and stricter implementing rules and regulations to defer unpredicted future consequences on economics [8], social and psychological aspect [9], and business operations [10] to cite a few. The kind of a cybersecurity program logic model (CPLM) that is tailored fit to the Philippine higher education institutions (HEI) crafted based on the lived experiences of the respective HEIs expert informants (IT officers).

The output of the study is of benefit to the Department of Information and Communication Technology-Cybersecurity Bureau, to higher education authorities like the Commission on Higher Education (CHED), Civil Service Commission, the Department of Budget and Management (DBM), and the Philippine Association of State Colleges and Universities (PASUC), to include SUCs in crafting a PLM. A standardized cybersecurity model as a basis for policy implementing rules and guidelines that protect confidential information and infrastructure thereby avoiding breaches of cyberattacks and financial losses on the part of the affected entity. Cybersecurity involves protecting information by preventing, detecting, and responding to cyberattacks. It not only stands with criminal activities dealing with computers and networks but also includes traditional crimes organized using the internet [11]. In the process of ensuring the security, integrity, confidentiality, and availability of data [12].

A comparative analysis [13] about the two African nations (Rwanda and Tunisia) to investigate the posture of governments regarding cybersecurity threats from a general perspective. Tagert [13] calls for localized strategies on cyber-defense which are appropriate to the developing countries benchmarked from the countries with well-defined cyber security mechanisms. This was because the author found out that developing countries have a high tolerance for cyber security breaches.

In the Americas, a qualitative study that assesses the national cybersecurity readiness of Jamaica recommends the adoption of international best practices [14]. In terms of incident response, Computer Emergency Response Team Coordinator Center (CERT/CC) presented cases studies of Columbia and Tunisia. A Colombia case study points out the processes of creating a national computer security incident report team (CSIRT) and summarizes lessons learned. The said learning highlights the vision of the government to support the creation of the team and coordination with the academe. Likewise, Tunisia utilizes a successful national CSIRT employing open-source tools in aid of overcoming resource restrictions. In the Latin American context, a report from OAS-Symantec [15] identifies trends, best practices guidelines for firms, and national efforts toward improving cybersecurity in every country. The national cybersecurity department according to the OAS-Symantec [15] proposed that the Latin American context has a national CSIRT, national cybersecurity governance affairs, awareness campaigns, a cybersecurity policy, a program for CIP, and international collaboration capabilities. This OAS report is purported to ensure awareness and does not address deep.

Hasib [10], a cybersecurity expert, articulates that cybersecurity is a business strategy; consequently, wanting a governmental-wide approach to execute proficiently. Currently, cybersecurity is perceived to be a business strategy, proactive cybersecurity leaders and expert information technologists are engaging in collaborative functions in training, and mentoring, and encouraging everyone's role to protect information leakage due to task saturation [16]. It is important that there should be a preparation to ensure a quick response for the cybersecurity attacks, a need for leadership for various security preparedness to counteract future cyber threats [17]. Many organizations promote technical training and transfer of learning to direct leadership competencies [16]. However, professional competence is not the same as organizational leadership but a leadership role in combating cyber [18].

Facing cybersecurity challenges requires individuals with a profound knowledge to detect, mitigate and respond to any cyber threats for the protection of pertinent data information. Hence, every nation has designed approaches to develop community awareness, including user education, cloud security, information security strategy, and unsecured personal devices. These challenges faced by SUCs are an opportunity to help improve its models, policies, and guidelines for securing critical infrastructure.

Since there were no plantilla positions for cybersecurity specialists in SUCs and in every agency in the government, the concerned institution created their Management Information System (MIS) unit to work and lower the fraction of cyber-attacks. One of the issues in the MIS in higher education is information security on "Big Data Analytics" [19]. The importance of informed choices for the information technologist is to consider the protection of the information-related program of the respective education sectors. Aside from a costly information breach affecting higher education, Reuter Staff, has found out that the consequence of incidents in information breach in corporate firms entails cost. Similar studies of the impact of information breaches requiring cost for security were proved by previous studies [8], [20], [21]. Cleveland [17] also included in their study on the cybersecurity framework the vulnerability to cybersecurity hacking were energy sectors, critical manufacturing, water systems, and commercial facilities.

Higher education is among those which have a higher rate of cyberattacks [22]. Every SUCs, even all the agencies in the government and private institutions must give time to communicate, inform and send out emails and text brigades to warn faculty, staff, students, and employees of any possible cyber-attack or phishing email that may be circulating. Not only has the MIS departments/unit faced the challenge of educating students, faculty, and staff about cyber-security awareness. There will be campaigns that drive students full-time to attend awareness programs that are included in the curriculum to make it successful. Al-Janabi and Shaourbaji [23] emphasized the importance of campaign awareness in combating cyber-attacks. Clientele like students, staff, and faculty, parents must recognize potential risks and dangers, and every MIS department/unit of every higher educational institution and agencies in the government must lead in educating the people with their available resources. Simple signs sometimes neglected by users that they need to be aware of indicating a phishing attempt are in misspelled words, the degree of importance or deadlines, imitated names along with false web links, and the request of personal information like usernames and passwords, account identification and credit account number [24]. Users must be watchful and mindful of the signs of a possible breach, and this will only happen if our personnel in charge in the MIS departments/unit can transcend the challenge of educating all students, staff, faculty, and all personnel.

Since the Philippines is a developing nation, it just only addresses some aspects of cybersecurity strategies and capacity building, but there were no inclusion of cyber-education for children, and no specific areas of courses that focus on cyber-teaching, and regional cybersecurity practices [25]. This provides an informed national strategic response for developing nations, especially on cybersecurity threats. The government needs to develop rigorous cyber-security guidelines and policies, to give user education training on the do's and don'ts of user behavior, and need to enforce strict implementation [26].

Seuring and Muller [27] advised that there were areas in which developing countries find challenges crafting cyber capacity strategy. It includes institutional stability, building knowledge, legal framework, and private sector engagement. The government should consider factors like capabilities to practice said strategies at the right time when adopting best practices from other developing countries.

There were suggestions to include identifying indicators, allocation of resources, and forming a plan with sharing of responsibilities. Jansson and Solms [28] proposed a cyber-safety curriculum for children (based on films and videos) in order to train, educate and help these individuals protect their privacy on the Internet (e.g., emails, social media, and social network sites like Facebook, Instagram, and Twitter). Furthermore, providing children the knowledge, information, and skills on how to defend against threats and phishing attempts has been demonstrated to be effective. In terms of cloud computing, Butler [29] introduced new information security that is at risk like social media, and mobile devices.

There are security issues in cloud security, challenges in cloud computing that have been classified into four areas consisting of access control, cloud infrastructure, network, and data security [30]. Cloud computing before it grows experiences challenges to its benefits to improve its network security while hacking and

intrusion increase. When authorized users are having access to the cloud through the internet it raises the risks for security. The cloud-computing infrastructure includes cloud service models that relate to virtualization settings, which is dangerous due to the multi-user shared environment. Data security carries the 24 hours utmost risk due to MIS departments/units storing information in a remote cloud [30]. Since there were many security challenges mentioned, MIS departments/units need to evaluate the current resource being utilized and how accurate they are to prevent data breaches.

Cloud computing which is chartered from a private entity is being operated by someone who is anonymous to the customer. There is a need for a third-party provider to preserve the data in the cloud which is one of the most uncertain tasks. The cloud-computing client only wishes to trust and depend on their data security to a mysterious source data regulator. Due to this activity, there is a big opportunity for cyber-terrorist to include insiders who may be a member of the third-party vendor or a possibility of the third-party vendor compromising data security without the knowledge of the owner of the data. In relation to this, there is no clear discussion on cloud-computing data storage policy or cloud data security [31].

Cloud-computing is susceptible to cyberattacks as vast amounts of data are being deposited in the cloud along with its identities and locations and would be aware of safety compromises unless they come to know about the victimization they have gone through. Stealing passwords in the clouds are way too easy through phishing and other social engineering techniques [32]. Technically, cloud-computing is prone to insider attacks. A discontented employee having known of the account could share information with another account. The cloud-computing makes this difficult 10 times damaging since organizational access to the cloud management platform enables access to copy and sneak any simulated machine, undetected, as well as potentially obliterate the entire cloud environment in very short order [33].

The lack of standardization of cloud-computing is a huge problem. There are no standard norms or legal requirements that regulate the cloud providers, to ensure safety, ensure data storage. Because of these reasons, cloud-providers may have employed inexperienced cybersecurity to take charge and disregard its objectives to cyber-safety. There is a high risk of hiring a member of a cyber-terrorist organization or individual to provide information from them, steal and/or damage the data and even hack the critical information infrastructure in the future. Cloud computing offers a reduction of the cost of protecting information security [34]. However, the vulnerability of insider cyber-attack is at risk. One employee uses another computer, and even uses another's external drives. Another example of a cloud-computing application that uses Duo security as two-factor authentication that protects PeopleSoft applications to ensure unified security for students, staff, and faculty in higher educational institutions. Thus proper adoption, application, and technology utilization in education plays a vital role in the protection of learning information [35].

One of the greatest challenges to information security strategy is staffing and funding, and to become effective is not to depend on technological measures, but on non-technical activities such as strict implementation and compliance with standard and correct security practices [29]. Universities and colleges are at risk for information security breaches [29]. Higher educational institutions and all types of organizations have the least secured environments in safeguarding MIS [36].

Catota, Morgan, and Sicker [37] noted that it is an advanced technology strategy to use like Scanners, Intrusion Prevention System (IPS), Intrusion Detection System (IDS). Other researchers [11] suggested the application Firewall. Information security solutions/technologies do not offer a solution to application-level threats. Internal networks are only protected by the network firewalls. But, still vulnerable to various application threats. The reason is briefly explained along with the limitations [11]: i) Vulnerability Scanners is an automated tool and its purpose is to crawl into web applications by checking its web pages and finding the vulnerabilities in its application using the passive technique. This strategy is to generate scanned probe inputs and check their responses against these inputs for security vulnerabilities; ii) IPS is designed to detect unauthorized access of resources and prevent these resources from any unauthorized access; iii) IDS is internet-based software applications that catch unauthorized access to network systems. A signature-based detection system employs pattern-based matching algorithms for data breaches. It established malicious input against the original profile in the database in the case of the Anomaly-based systems. While data mining is a framework detection pattern that provides reports on malicious attacks through statistical techniques. Another system for IDS is ontology-based solutions used in information security. Raskin *et al.* [38] developed the ontology for data integrity of web resources and advocate the use of ontology for information security strategy. The perspective of information security is "illustrated the model's assets, threats, vulnerabilities, countermeasures, and their relations" [38]. This shows that there is existing research focusing on the utilization of information security ontology that can support the ISO/IEC 27001 [11].

In the study of Cybersecurity Awareness in Higher Education [24], cybersecurity threats are not only common with computers and networks. These threats are becoming increasingly popular in gadgets specifically mobile devices. This is something that the academic community should be aware of. This setback is a need to be addressed by SUCs and in higher education in general [39]. Patten and Harris [39] implied that "Various security threats that are associated with computers are also associated with mobile devices. Nonetheless, mobile

devices pose more threats and challenges when it comes to protecting your information because your gadget and mobile phones typically store more personal data than your computer does. Moreover, smart mobile devices constantly moving in and out of Wi-Fi networks, many of which are not safe, and make stealing data easier for hackers. Another challenge with mobile device security is the amount of malware accessible and can be downloaded from the App Store for free. Malware on mobile devices is now higher than it is for PCs.”

Policy on the entry of faculty and student gadgets is implemented in some universities. In the case of bringing your own device (BYOD) in school, Raths [40] found that it would be an advantage of enhancing learning collaboration and mobility in the workplace. Further, Raths [40] pointed out that it could also give complicated issues on personal information and data leakage. In the case of the University of California, BYOD policy was implemented by information technology experts to secure the vulnerability of data attacks [41].

The theoretical framework for this study is embedded in the constructivist approach [42] on the dispersion of innovations theory. According to previous researchers [43], [44], the constructivist inquiry is consistent with qualitative methods. Qualitative research aims to understand what people believe and feel as well as how they interpret events [29], [45], [46]. Consistent theories in ICT and information security are not common, Rogers *et al.* [42] dispersion of innovations theory may provide a compact theoretical foundation for learning areas in this field [47]. Rogers *et al.* [42] theory endeavors to justify and forecast how improvements in ICT evolve over the information system that can provide awareness to prioritize enhanced pervasiveness of interconnected devices attached to the IoT and their impact on the proliferation of information security threats among SUCs. Additionally, the theory will shed light on whether the higher academic institutions employ safer information security practices that are capable of addressing data breaches.

Rogers *et al.* [42] diffusion of innovations theory is applicable for the purpose of this study in that it provides a means for understanding the technology adoption process. This theory may help identify perceptions of the technical, social, organizational, and other factors contributing to the high number of information security incidents in higher education. Secondly, the theory may explore security features contributory to adopting the technologies and practices in the respective higher institutions.

## 2. RESEARCH METHOD

The current research utilized a multiple case study that is highly qualitative in nature. The study explored cybersecurity threats and challenges among SUCs being the current subject of malicious online threats on crucial information data stored in a digital system. Expert informants (IT officers) were purposively selected. These IT Officers have hands-on experience with potential cybersecurity threats. They are those who are active and pro-active to develop information security resources in their respective institutions as Table 1.

Table 1. Expert informants from selected higher educations in the Philippines

	Name of SUC	No. of cybersecurity informants
1.	Philippine Normal University (PNU)	1
2.	Eulogio “Amang” Amang Rodriguez Institute of Science and Technology (EARIST)	1
3.	Marikina Polytechnic College (MPC)	1
4.	Philippine State College of Aeronautics (PhilSCA)	1
5.	Polytechnic University of the Philippines (PUP)	1
6.	Rizal Technological University (RTU)	1
7.	Technological University of the Philippines (TUP)	1
	Total number of informants	7

The validated semi-structured survey interview instrument with open-ended questions was used to solicit participants’ or expert informants’ in-depth descriptions about their lived experiences. The interviews will follow the seven stages of interview investigation as depicted by Brinkmann and Kvale [48]: thematizing, designing, interviewing, transcribing, analyzing, verifying, and reporting. Thematizing involves clarifying the overall purpose of the investigation. A sort of data validation from the interview with the IT officers were also validated through a triangulation method utilizing the transcribed interview responses, from the literature readings, and gathered data reports [49].

For the seven-cybersecurity informant in the SUCs, the questionnaire was made in phases. There was an individual discussion during the interview with naturalistic observation procedures of the phenomenon under investigation [43]. Naturalistic observation entails participants in their normal setting without any manipulation or stimulation on the part of the researcher [44].

### 3. RESULTS AND DISCUSSION

Without proper education and adequate knowledge, understanding, comprehension, and skill, users tend to be hesitant and intimidated to use and adopt these new strategies. The conduct of seminars, forums, training, and orientation is the best way to educate users in their individual institutions. Specialized training, certifications, and further studies are needed for the information security officers to become more confident in giving correct and mindful Information. Through this kind of program, vulnerability will be lessened because of a lack of information to the user. There will be a low level of incidence for the older faculty to share or give their username and passwords that assist them in the encoding of grades. The two participating colleges will commence their target of establishing their MIS unit and make the proposed programs into action. Another participating college also mentioned that information about the use of free Wi-Fi is only given to IT students only but further suggested that it must be carried out to all members of the community.

According to the expert informants, every user has allotted space for cloud-based emails such as Gmail that helps reduce information security threats and support costs [8]. On the other hand, another informant mentioned that having email hosted offsite, takes some of the burdens and risk-off their services and systems. A supplement firewall protection with IDS and client end-point security against malware, worms, and viruses. According to Panko [50], firewalls that filter traffic based on static rules, IDSs work by inspecting traffic for known signature patterns or anomalies differing from normal patterns. Also mentioned in the investigation was to include a cloud computing establishment for the MIS unit. However, it was found out that cloud computing was not a priority because it is costly [8]. One of the expert informants said:

*“Procurement of IT equipment in the government agencies, state universities, and colleges are done through public bidding as set by bids and awards committee. Moreover, some of them were packaged with free software and training. Certifications are needed but because of limited budget and high cost, it is not being prioritized by the management. The need for access to security equipment is necessary to support such initiatives that were reported to be very expensive. The reason that participating SUCs found to have no support for training leading to cybersecurity certifications. Informants indicated that they have not even considered such initiative for security.”*

Expert informants elucidated that their institution has an external network connected to the internet. Traffic from the internet and external systems are blocked from reaching internal systems with the use of their firewall. According to them, external network routers are connected to the internet. Internal and external systems controls are blocked by firewalls to protect the internal systems. According to the participants, external systems are equipped with firewalls to support the internal system without accessing the internal systems and other public computer devices. The participants also mentioned that authentications and registration methods work to counter malicious attacks, prevent hackers from entering the database system, use logs as signals for a security breach. As suggested by the informants, Hayes *et al.* [51] and Morrison *et al.* [52] logic model has proven to be a successful tool for program planning as well as implementation and performance management in numerous fields, including primary care. It is an efficient tool that requires little resources other than personnel time [53].

Logic model according to Bienkowski [54] is related to data mining and analytics. It requires human interventions for patterns of data protections, designs for best application tools, and ensures safety features of information access. McCawley [55] depicts the logic model process as a tool that has been used for more than 20 years by program managers and evaluators to describe the effectiveness of their programs. The logic model illustrates a sequence of cause-and-effect relationships, a system approach to communicate the path towards the desired result [55]. Many evaluation experts agree that the use of the logic model is an effective way to ensure program success [56]. Using a logic model to ensure program success helps develop systematic program management, planning, and evaluation of functions and control mechanisms. While cybersecurity is becoming a greater issue this time of pandemic the IoT and the pandemic brought about by the COVID-19, informants described some less serious incidents. According to one informant:

*“Due to limited information and awareness of the workers who all use the same generic login that other staff use a.k.a “default username and password”, there was one administrative staff in the registrar’s office who somehow realized that her account was being accessed by unknown user who try to gain access and disrupt her functions of using her own account. While this was not the result of a malicious attack or breach, the person in-charge still notified the affected user that her personal username and password has been exposed or attempted accessed, the informant explained.”*

Moreover, IT directors automatically shut down external systems upon detection of unauthorized access from outside networks that are attempting to access the external systems. Attempts of a system breach, defacement of websites, cyberbullying, and hacking of social media accounts were the most common experiences by the participating selected SUCs. According to Luo and Liao [57], the most common types of cybersecurity information threats involve malware, DDos, script kiddies, pop-ups, phishing accounting for 64.9% of attacks. The internet and email have provided an auspicious location for the increase of self-replicating nasty programs such as worms, malware, Trojan horses, and viruses [58].

Among the seven participating SUCs, there are only two SUCs that have the infrastructures, technology, and software. Installation of firewall, client endpoint, and antivirus were among the preparations being made to support, maintain the smooth business operations of these institutions. However, there is one college that has minimal preparation because the system employed is in local mode and there were plans to upload them online. Nonetheless, the two participating colleges have no definite infrastructures, technology, and software and are planning status to establish and implement their own MIS that will handle the operations, maintenance support, and back-up of important information and data.

There were numerous attempts of a system breach, defacement of websites 24 hours a day seven days a week and according to one participating state university they handled an average of 25 direct denial of service or what we call DDos but because of their continued upgrading of system maintenance and strict monitoring they are eliminating such threats to the lowest level. There was a mention also of cybersecurity using hack accounts by sending lewd messages, pictures, and videos to the connected friend's list of users. Expert informants also mentioned their experiences of pop-ups, script kiddies, and BOT hacking tools that are trying to penetrate their defenses wall and intrude on their data. Excerpt of the interview from one informant IT director:

*“Cybersecurity threats are just like a balloon that if you try to fill in more water on it the bigger it gets and that is data critical information. Hackers/hacktivists, cyber-criminals, and other cyber terroristic activity were trying to blow up to get the information they wanted. At first, they use needles to make a hole and then penetrate not only once but hundreds, thousands, or even a million times. Despite that we try to cover those pinned needles using practical ways by covering using our hands, however, there was a limitation to that so other methods like inserting tape or putting bubble gum will cover and that data will not be exposed. Those kinds of judgment emerge only through experiences, by attending seminars, training, workshops, and coping up with new trends and upgrades that are badly needed to maintain the validity and efficiency of data.”*

SUCs have been experiencing the threats since their data or information were being uploaded online. However, the two participating SUCs rarely underwent this type of activity and one participating college never experienced that there were threats since the informants do not have full access to data or information of their institution. Hence, three of the SUCs that outsourced external enrollment system providers mentioned that there was no information of threats or incidence occurring which disclosed information about their institutions.

The consensus among all the participants or the expert informants was that internal information system users recorded by far on the prevalent threats to SUCs. It was explained that hackers were not that big of a threat, since every activity being done by internal or external users was being monitored through logs in the database system. On the other hand, 85% of internal users account for the overwhelming majority of security problems.

Another way of possible threat to information security is by using share accounts or passwords. Some administrators and employees shared passwords with their colleagues whom they trusted, and sometimes among student assistants of the unit who assist them in the encoding of grades. Also mentioned was the average of 25 attempts of website defacement, but, since they are monitored there is no success on it.

This study involved an embedded multiple case study imperatively to enhance understanding the issues encompassing cybersecurity threats, challenges, and strategies among higher educational institutions from the perspectives of the participating state universities and colleges IT experts [42]. Due to the limited availability of relevant data on cybersecurity among SUCs, this study was purely exploratory in nature [59] in symmetry to disclose in-depth information about the topic [60], [61]. Also, this non-experimental study examined the threats, challenges, incidence, practices, and advanced strategies in relation to cybersecurity among selected SUCs as perceived and described by the IT expert participants.

In the current study, it appears that there is a gap in the literature identifying and understanding the cybersecurity threats and challenges among selected SUCs. The findings in this research study suggest that none of the SUCs have a position dedicated to cybersecurity or information security, instead of IT faculty or personnel who are teaching information security-related courses, or programmer and with other secondary

responsibilities such as internal information system users, designated end-user as member of Bids and Awards Committee, network and server administration. This is consistent with previous study [8], that internal information user poses a prevalent threat to institutions. Employee non-observance to information security policies poses a drawback to threats, challenges, and incidence [62].

Nevertheless, the findings of this indicated that there is an incident unique to selected SUCs because their individual mandate, vision, mission, and objectives are not necessarily consistent with much of the literature. Malicious hacking attacks on information breaches are usually caused by human error. Furthermore, Garrison and Ncube [63] stated that “insider incidents or those carried out internally are less frequent than those initiated externally.”

The result of this study illustrates the readiness of participating SUCs that installation of firewall, client-endpoint security, and antivirus helped, prevent in protecting these institutions. The attempts of system breach [63], [64], defacement of websites [65], cyberbullying, and hacking of social media accounts [66] was one concern of security incidents among SUCs. Whereas there is certain literature suggesting that hackers are the primary threat to information security systems, Lou and Liao [57] as well as Myyry *et al.* [62] the apparent risk of hacking appears to be minimal at other participating colleges due to no internet connection and out-sourcing of enrollment systems. Luo and Liao [57] further suggested that firewalls, virtual private networks (VPNs), and access controls are used in response to cybersecurity information threats.

Information channels usually targeted by the cybercriminals were the enrollment system, through access in printer and server and software. Interconnected devices become gradually persistent and formidable in the propagation of infection of malware, autorun universal serial bus (USB) virus, worms, and Trojan viruses [67]. The unauthorized access of students using faculty accounts, account ID does not have passwords, and defacement of websites were common incidences encountered by the participating state universities. The expert informants identified the vulnerabilities of the following critical information of their respective academic institutions. The detail of the threats and problems is presented in Table 2.

Table 2. Philippine HEIs cybersecurity threats

Characterization	Subcategory
1. Cybersecurity of information	<ul style="list-style-type: none"> <li>- Creation of a unique cryptographic algorithms</li> <li>- Protection from cyber-threats, malware and virus</li> <li>- Security of local and wide area network</li> <li>- Security of gadgets and cellphones</li> <li>- Security in social media</li> <li>- Measures to deter threat in accessing data</li> <li>- Illegal act of accessing computer network systems</li> <li>- Prevention from intruders to access databases</li> </ul>
2. Readiness	<ul style="list-style-type: none"> <li>- Installation of firewall, client end point and anti-virus</li> <li>- Very minimal because systems are not online</li> <li>- No internet accesses</li> <li>- No issues, not hook online</li> <li>- Outsourcing of enrollment system</li> </ul>
3. Threats	<ul style="list-style-type: none"> <li>- Attempts of system breach</li> <li>- Defacement of websites</li> <li>- Cyberbullying in social media using other accounts</li> <li>- Hacking of accounts</li> <li>- Pop ups</li> <li>- Script-kiddies</li> <li>- Bot hacking tools</li> </ul>
4. Frequency	<ul style="list-style-type: none"> <li>- Every time</li> </ul>
5. Incidence	<ul style="list-style-type: none"> <li>- Unauthorized access of students using faculty accounts defacement of websites</li> <li>- Account id does not have passwords</li> <li>- No issues, use local accounts</li> <li>- No internet access</li> </ul>
6. Channels	<ul style="list-style-type: none"> <li>- Printer and server</li> <li>- Enrollment system</li> <li>- Software's</li> </ul>
7. Infection	<ul style="list-style-type: none"> <li>- Malware</li> <li>- Autorun USB virus</li> <li>- Worms</li> <li>- Virus</li> </ul>

The results of this study supported the argument of Hasib [10] that cybersecurity affects business operations in bugging down of connections, alteration of data, and disruption of business operation among financial and administrative functions such as accounting, cashier, admission, and registrar is considered critical. According to Panko [50], internal users can pose a serious threat and cause widespread harm because



these individuals may have access to systems or have extensive knowledge about how the system works. Insiders may be familiar with the policies, procedures, and applications used for protecting information systems in the organizations. This may allow firsthand knowledge about the organization’s information systems flows, procedures, and activities in networks or systems, allowing insiders to bypass security measures designed to prevent unauthorized access [68].

The diffusion of innovations framework [42] may help provide insights into the understanding of the cybersecurity information strategies but may not be enough to prevent further incidents. The study suggested that observed comparative study, best practices influence acceptance of the security management strategies and cybersecurity information protection. However, the prevalence of cybersecurity breaches experienced by those higher institutions and other government agencies paved the way for the academic institutions to protect their respective information databases which could lead to more damaging results on the lost physical drive files like financial records, enrolment databases, research results, and damage to institutions websites. The results of this study support the assertion that relative advantage, uniqueness, compatibility, trialability, and observability, are positively related to adoption rates, while complexity is negatively related to adoption [42]. Moreover, Rogers *et al.* [42] diffusion of innovations the framework may help provide awareness into what may be impeding ideal advanced cybersecurity strategies. In addition, difficulties, and intricacies of cybersecurity guidelines, not present or roadmap relating to information security strategies may also be an impending role. For instance, efforts of the selected SUCs do not show characteristics of strong compatibility on cybersecurity norms, practices, and culture, the need to adopt successful mitigation practices, or a framework that other higher educations and government institutions are using.

Various proposed cybersecurity has been initiated in the HEIs as cited in the literature and the responses gathered from the study expert informants but none of which are able to put in place a roadmap to mitigate cybersecurity threats. It is for this reason that researchers find it a high time to propose the PLM as presented in Figure 1. It is crucial in aid of protecting the critical information by sustaining the value of the effort, talent, time, and cost that our higher education authorities have invested to keep us, and the future generation informed of the foundations of the body knowledge that made us who we are today.

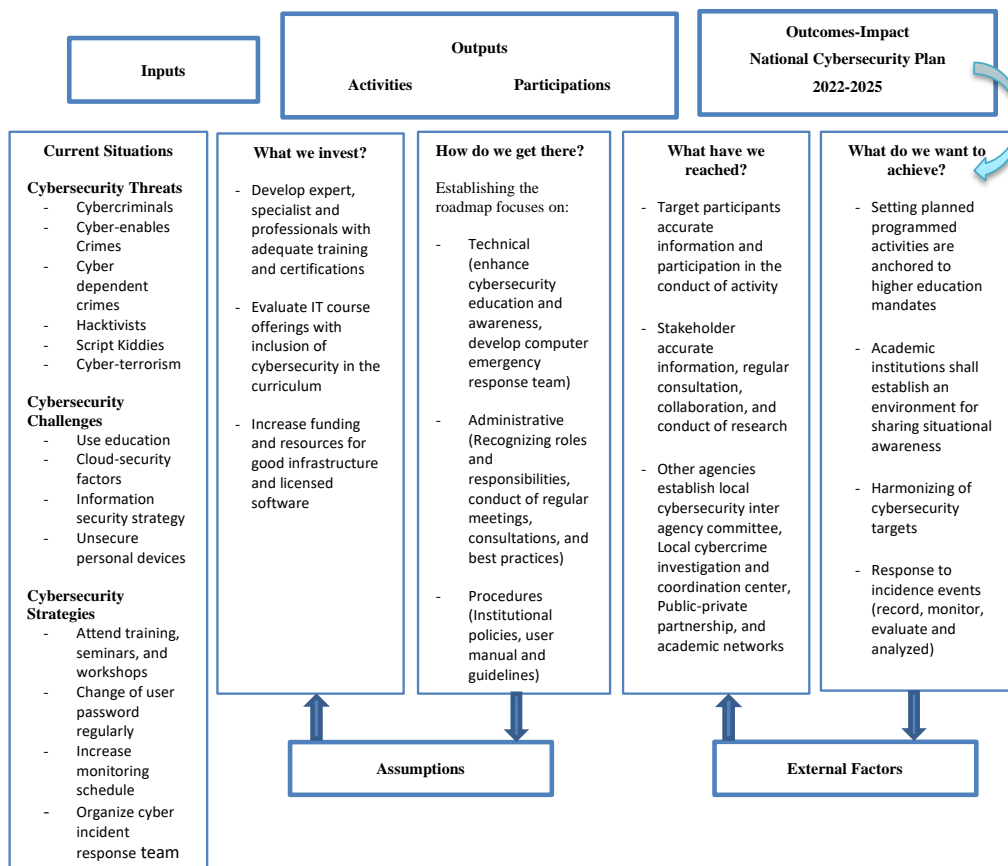


Figure 1. HEIs cybersecurity program logic model

#### 4. CONCLUSION

Overall, the findings of the study revealed that cybersecurity, readiness, threats, frequency, incidence, channels, and infection are the indications of a cybersecurity breach. Hence, a PLM of the current study is framed from the prior theories, literature, and the current experiences of the expert informants. It has the aim of addressing the prevalence of cybercrimes in the Philippine Higher Education System.

The researchers recommended that educational institutions should prioritize the necessity of information protection. Insights of the researchers and the current study result would likewise update every one of the vulnerabilities of the retained online information especially that we are now in the age of the IoT and the current situation of the COVID-19 pandemic which heightened the need of online activities. In contribution to the body of knowledge, this research can be utilized by other investigators on academic-related cyber infringement.

#### ACKNOWLEDGEMENTS

The authors would like to acknowledge the Technological University of the Philippines (TUP) and the Philippine Normal University (PNU) Management and Officials for the approval of the conduct of this research study.

#### REFERENCES




- [1] M. Dunn Cavelty and A. Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science," *Contemporary Security Policy*, vol. 41, no. 1, pp. 5–32, Jan. 2020, doi: 10.1080/13523260.2019.1678855.
- [2] D. Benoliel, "Towards a cybersecurity policy model: Israel national cyber bureau case study," *The North Carolina Journal of Law & Technology*, vol. 16, no. 3, pp. 435–485, 2015.
- [3] Republic of The Philippines, "Republic Act No. 10175: An Act Defining Cybercrime, Providing For The Prevention, Investigation, Suppression And The Imposition Of Penalties Therefor And For Other Purposes," The Lawphil Project, 2012. [Online]. Available: [https://lawphil.net/statutes/repacts/ra2012/ra\\_10175\\_2012.html](https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html).
- [4] M. D. Richardson, P. A. Lemoine, W. E. Stephens, and R. E. Waller, "Planning for cyber security in schools: the human factor," *Educational Planning*, vol. 27, no. 2, pp. 23–39, 2020.
- [5] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide: Recommendations of the national institute of standards and technology," Gaithersburg, MD, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.
- [6] I. M. Venter, R. J. Bignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's,'" *Heliyon*, vol. 5, no. 12, p. e02855, Dec. 2019, doi: 10.1016/j.heliyon.2019.e02855.
- [7] Republic of The Philippines, "National Cybersecurity Plan 2022," Department of Information and Communications Technology, 2022. [Online]. Available: <https://dict.gov.ph/national-cybersecurity-plan-2022>.
- [8] S. Carmody *et al.*, "Building resilient medical technology supply chains with a software bill of materials," *npj Digital Medicine*, vol. 4, no. 1, p. 34, Dec. 2021, doi: 10.1038/s41746-021-00403-w.
- [9] M. Bada and J. R. C. Nurse, "The social and psychological impact of cyberattacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*, Elsevier, 2020, pp. 73–92. doi: 10.1016/B978-0-12-816203-3.00004-6.
- [10] D. M. Hasib, *Cybersecurity Leadership: Powering the Modern Organization (Global Cybersecurity Thought Leader)*. CreateSpace Independent Publishing Platform, 2014.
- [11] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, Mar. 2013, pp. 1–6. doi: 10.1109/ISADS.2013.6513420.
- [12] T. H. Bhat and A. A. Khan, "Cybercrimes, security, and challenges," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 5, pp. 509–513, 2015, doi: 10.17148/IJARCCCE.2015.45108.
- [13] A. C. Tagert, "Cybersecurity challenges in developing nations," Carnegie Mellon University, 2010. [Online]. Available: [repository.cmu.edu/cgi/viewcontent.cgi?article=1021&context=dissertations](https://repository.cmu.edu/cgi/viewcontent.cgi?article=1021&context=dissertations).
- [14] K. P. Newmeyer, "Cybersecurity strategy in developing nations: A Jamaica case study," Walden University, 2014.
- [15] S. Caponi, "Cybersecurity trends for 2014," *Cybersecurity, Governance*, 2014. [Online]. Available: <https://www.corporatecomplianceinsights.com/cybersecurity-trends-for-2014/> (accessed Feb. 21, 2014).
- [16] D. N. Burrell, A. S. Aridi, and C. Nobles, "The critical need for formal leadership development programs for cybersecurity and information technology professionals," in *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, 2018, vol. 2018-March, pp. 82–91.
- [17] S. Cleveland and M. Cleveland, "Towards cybersecurity leadership framework," in *Thirteenth Midwest Association for Information Systems Conference*, 2018, pp. 1–5.
- [18] D. L. Lester and M. Tennessee, "The desktop manager," *Advanced Management Journal*, vol. 71, no. 4, 2006.
- [19] B. Daniel, "Big data and analytics in higher education: Opportunities and challenges," *British Journal of Educational Technology*, vol. 46, no. 5, pp. 904–920, Sep. 2015, doi: 10.1111/bjet.12230.
- [20] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security*, vol. 11, no. 11, pp. 431–448, 2003.
- [21] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, pp. 70–104, Oct. 2004, doi: 10.1080/10864415.2004.11044320.
- [22] J. Alcon "13% Of The Higher Education Sector Has Been Infected With Ransomware," Bitsight.com, 2016. [Online]. Available: <https://www.bitsight.com/blog/higher-education-infected-with-ransomware>.
- [23] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in the educational environment in the middle east," *Journal of Information & Knowledge Management*, vol. 15, no. 01, p. 1650007, Mar. 2016, doi: 10.1142/S0219649216500076.
- [24] T. Hunt, *Cyber security awareness in higher education*. 2016. [Online]. Available: <https://core.ac.uk/download/pdf/51141415.pdf>.

- [25] K. P. Newmeyer, "Elements of national cybersecurity strategy for developing nations," *National Cybersecurity Institute Journal*, vol. 1, no. 3, pp. 68–70, 1377.
- [26] D. F. Norris, L. Mateczun, A. Joshi, and T. Finin, "Cybersecurity challenges to American local governments," in *Proceedings of the European Conference on e-Government, ECEG*, 2017, vol. Part F1294, pp. 110–117.
- [27] S. Seuring and M. Müller, "Core issues in sustainable supply chain management - a Delphi study," *Business Strategy and the Environment*, vol. 17, no. 8, pp. 455–466, Dec. 2008, doi: 10.1002/bse.607.
- [28] K. Jansson and R. von Solms, "Phishing for phishing awareness," *Behaviour & Information Technology*, vol. 32, no. 6, pp. 584–593, Jun. 2013, doi: 10.1080/0144929X.2011.632650.
- [29] R. D. Butler, "An examination of issues surrounding information security in California colleges," 2013. [Online]. Available: <http://search.proquest.com/docview/1473920430?accountid=44888>.
- [30] K. H. A Al-Shrouf, F. M. A Al-Shrouf, M. R. Hassan, and A. -Jordan Hassen Fajraoui, "Cloud computing security challenges in higher educational institutions-A survey," *International Journal of Computer Applications*, vol. 161, no. 6, pp. 975–8887, 2017, [Online]. Available: <https://pdfs.semanticscholar.org/e3f7/21c6708e29156096cb6b5e55ac4ce8571293.pdf>.
- [31] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?" *Journal of Information Technology & Politics*, vol. 5, no. 3, pp. 269–283, Oct. 2008, doi: 10.1080/19331680802425479.
- [32] A. Khan, "Preventing phishing attacks using one time password and user machine identification," *International Journal of Computer Applications*, vol. 68, no. 3, pp. 7–11, 2013, [Online]. Available: <http://arxiv.org/abs/1305.2704>.
- [33] S. Latha, L. Jianhong, and W. John, "Cyber-Terrorism and Cyber Security: A Global Perspective," in *Justice Report*, 2016, pp. 1–9.
- [34] A. Duncan, S. Creese, and M. Goldsmith, "An overview of insider attacks in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 12, pp. 2964–2981, Aug. 2015, doi: 10.1002/cpe.3243.
- [35] W. Kekahio, B. Lawton, L. Cicchinelli, and P. Brandon, *Logic models: A tool for effective program planning, collaboration, and monitoring*. Washington, DC: U.S. Department of Education, Institute of Education Sciences, National Center for Education Evaluation and Regional Assistance, Regional Educational Laboratory Pacific, 2014. [Online]. Available: <https://www2.ed.gov/about/offices/list/oese/oss/technicalassistance/easlogicmodelstoolmonitoring.pdf>
- [36] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Computers & Security*, vol. 27, no. 7–8, pp. 241–253, Dec. 2008, doi: 10.1016/j.cose.2008.07.008.
- [37] F. E. Catota, M. G. Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the Ecuadorian financial sector," *Journal of Cybersecurity*, vol. 4, no. 1, Jan. 2018, doi: 10.1093/cybsec/tyy002.
- [38] V. Raskin, C. F. Hempelmann, K. E. Triezenberg, and S. Nirenburg, "Ontology in information security: A useful theoretical foundation and methodological tool," in *Proceedings New Security Paradigms Workshop*, 2001, pp. 53–59.
- [39] K. P. Patten and M. A. Harris, "The need to address mobile device security in the higher education IT curriculum," *Journal of Information Systems Education*, vol. 24, no. 1, pp. 41–52, 2013.
- [40] D. Rath, "Crossing the device divide: With the help of browser-based software, students in BYOD districts can be on the same page even if they have different devices," *T.H.E. Journal Technological Horizons in Education*, vol. 40, no. 5, p. 9, 2013.
- [41] H. V. Nguyen, "Cybersecurity Strategies for Universities with Bring Your Own Device Programs," Walden University, 2019. [Online]. Available: <https://search.proquest.com/docview/2329729362?accountid=17242>.
- [42] E. M. Rogers, A. Singhal, and M. M. Quinlan, "Diffusion of innovations," in *An Integrated Approach to Communication Theory and Research, Third Edition*, 3rd ed., 2019, pp. 415–433. doi: 10.4324/9780203710753-35.
- [43] A. Suhendi and P. Purwamo, "Constructivist learning theory: The contribution to foreign language learning and teaching," *KnE Social Sciences*, vol. 3, no. 4, p. 87, Apr. 2018, doi: 10.18502/kss.v3i4.1921.
- [44] J. Corbin and A. Strauss, *Basics of qualitative research (3rd ed.): Techniques and procedures for developing grounded theory*, United States: SAGE Publications, Inc., 2008. doi: 10.4135/9781452230153.
- [45] G. Chowdhury, "Qualitative research for the information professional: A practical handbook (2nd ed.)," *Online Information Review*, vol. 30, no. 5, pp. 599–600, Sep. 2006, doi: 10.1108/14684520610706497.
- [46] R. K. Yin, *Case study research and applications: Design and methods*, 6a ed. vol. 53, no. 5. SAGE Publications, Inc., 2001.
- [47] E. G. Carayannis and E. Turner, "Innovation diffusion and technology acceptance: The case of PKI technology," *Technovation*, vol. 26, no. 7, pp. 847–855, Jul. 2006, doi: 10.1016/j.technovation.2005.06.013.
- [48] S. Brinkmann and S. Kvale, "Planning an interview study," in *Doing Interviews*, London EC1Y 1SP: SAGE Publications Ltd, 2018, pp. 39–56. doi: 10.4135/9781529716665.n4.
- [49] N. Carter, D. Bryant-Lukosius, A. DiCenso, J. Blythe, and A. J. Neville, "The use of triangulation in qualitative research," *Oncology Nursing Forum*, vol. 41, no. 5, pp. 545–547, Sep. 2014, doi: 10.1188/14.ONF.545-547.
- [50] R. R. Panko and J. L. Panko, *Business Data Networks and Telecommunications*, 7th ed. Upper Saddle River, NJ: Prentice Hall, 2008.
- [51] H. Hayes, M. L. Parchman, and R. Howard, "A logic model framework for evaluation and planning in a primary care practice-based research network (PBRN)," *Journal of the American Board of Family Medicine*, vol. 24, no. 5, pp. 576–582 7p, 2011, doi: 10.3122/jabfm.2011.05.110043.
- [52] C. Morrison, J. P. Lee, P. J. Gruenewald, and C. Mair, "The reliability of naturalistic observations of social, physical and economic environments of bars," *Addiction Research & Theory*, vol. 24, no. 4, pp. 330–340, Jul. 2016, doi: 10.3109/16066359.2016.1145674.
- [53] K. E. Luck, S. Doucet, and A. Luke, "The development of a logic model to guide the planning and evaluation of a navigation center for children and youth with complex care needs," *Child & Youth Services*, vol. 41, no. 4, pp. 327–341, Oct. 2020, doi: 10.1080/0145935X.2019.1684192.
- [54] M. Bienkowski, M. Feng, and B. Means, "Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics: An Issue Brief," 2012. [Online]. Available: <https://tech.ed.gov/wp-content/uploads/2014/03/edm-la-brief.pdf>.
- [55] P. F. McCawley, "The logic model for program planning and evaluation," University of Idaho, 2002.
- [56] W. K. Foundation, *Using logic models to bring together planning, evaluation, and action: Logic model development guide*. Michigan: Battle Creek, 1998.
- [57] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195–202, Sep. 2007, doi: 10.1080/10658980701576412.
- [58] J. Kinder, S. Katzenbeisser, C. Schallhart, and H. Veith, "Proactive detection of computer worms using model checking," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 4, pp. 424–438, Oct. 2010, doi: 10.1109/TDSC.2008.74.




- [59] K. A. Rendle, C. M. Abramson, S. B. Garrett, M. C. Halley, and D. Dohan, "Beyond exploratory: A tailored framework for designing and assessing qualitative health research," *BMJ Open*, vol. 9, no. 8, p. e030123, Aug. 2019, doi: 10.1136/bmjopen-2019-030123.
- [60] J. Winterton, "Business research methods," *Management Learning*, vol. 39, no. 5, pp. 628–632, Nov. 2008, doi: 10.1177/13505076080390050804.
- [51] L. Yeomans, "Qualitative methods in business research," *Action Learning: Research and Practice*, vol. 14, no. 3, pp. 298–301, Sep. 2017, doi: 10.1080/14767333.2017.1358600.
- [62] L. Myyry, M. Siponen, S. Pahlila, T. Vartiainen, and A. Vance, "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems*, vol. 18, no. 2, pp. 126–139, Apr. 2009, doi: 10.1057/ejis.2009.10.
- [63] C. Posey Garrison and M. Ncube, "A longitudinal analysis of data breaches," *Information Management & Computer Security*, vol. 19, no. 4, pp. 216–230, Oct. 2011, doi: 10.1108/09685221111173049.
- [64] K. F. Steinmetz, "Introduction: Technocrime at the margins," *Journal of Qualitative Criminal Justice & Criminology*, vol. 6, no. 2, Dec. 2018, doi: 10.21428/88de04a1.1d0b3f17.
- [65] C. J. Howell, G. W. Burruss, D. Maimon, and S. Sahani, "Website defacement and routine activities: considering the importance of hackers' valuations of potential targets," *Journal of Crime and Justice*, vol. 42, no. 5, pp. 536–550, Oct. 2019, doi: 10.1080/0735648X.2019.1691859.
- [66] G. M. Abaido, "Cyberbullying on social media platforms among university students in the United Arab Emirates," *International Journal of Adolescence and Youth*, vol. 25, no. 1, pp. 407–420, Dec. 2020, doi: 10.1080/02673843.2019.1669059.
- [67] D. Acarali, M. Rajarajan, N. Komninos, and B. B. Zarpelão, "Modelling the spread of botnet malware in IoT-based wireless sensor networks," *Security and Communication Networks*, vol. 2019, pp. 1–13, Feb. 2019, doi: 10.1155/2019/3745619.
- [68] D. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall, "Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1," Software Engineering Institute, Carnegie Mellon University, pp. 1–88, 2009.

## BIOGRAPHIES OF AUTHORS



**Noly M. De Ramos**    is currently the OIC of the Office of the Campus Registrar and Admissions at Philippine Normal University South Luzon, Lopez, Quezon (PNUSL). He has been elected as Auditor of Philippine Normal University Federation (PNUFed) and elected as Vice President of Philippine Normal University Faculty Association, Inc. (PNUFA). He is currently the Vice-Chair and member of the Bids and Awards Committee at PNUSL. He is a copy and style editors of LUKAD, An Online Journal of Pedagogy. His research interests include Technology and Livelihood Education, Gender and Development, Agri-Fisheries, Home Economics, and Industrial Education. He can be contacted at email: [deramos.nm@pnu.edu.ph](mailto:deramos.nm@pnu.edu.ph).



**Francisco Dente Esponilla II**    is an Associate Professor II of the College of Liberal Arts (CLA) of the Technological University of the Philippines (TUP). He has held office in concurrent capacity as a Research Specialist in the University Research and Development Services (URDS) since 2010. He is currently the assistant to the Vice President for Planning in the University Solid Waste Management, internal ISO reviewer, NBC 461 Zonal evaluator, and member of the procurements' Bids and Awards Committee (BAC). A regular member and a Board of Director of the Philippine Higher Education Research Consortium, Inc. His research interests include community development, gender and development (GAD), industrial education, economics and social sciences. He can be contacted at email: [Francisco\\_esponilla@tup.edu.ph](mailto:Francisco_esponilla@tup.edu.ph).