MITIGATING CYBER THREATS TO PHILIPPINE STATE UNIVERSITIES AND COLLEGES: A COMPREHENSIVE VULNERABILITY ASSESSMENT OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF SOUTHERN PHILIPPINES - CAGAYAN DE ORO CAMPUS ICT INFRASTRUCTURES

Mary Ann E Telen[1], Philip T. Abamonga[2], Tristan Paul Chua[3]
[1,2,3] University of Science and Technology of Southern Philippines, C.M. Recto Ave., Lapasan, Cagayan de Oro City, Philippines
*For Correspondence; Tel. +639265918458, Email: maryann.telen@ustp.edu.ph

***ABSTRACT** - This study aims to assess the cybersecurity vulnerabilities of the University of Science and Technology of Southern Philippines (USTP) Cagayan de Oro Campus and provide mitigation policy recommendations to address identified weaknesses. The increasing incidence of cybersecurity threats and attacks on academic institutions worldwide poses a significant challenge to higher education institutions, including Philippine State Universities and Colleges (SUCs). In response, this study conducted a comprehensive vulnerability assessment of USTP Cagayan de Oro Campus ICT infrastructures to identify areas of weaknesses and provide mitigation policy recommendations. The study used a combination of qualitative and quantitative research methods, including interviews, surveys, and network scanning tools, to assess the institution's cybersecurity posture comprehensively. The vulnerability assessment revealed significant cybersecurity vulnerabilities across the institution's ICT infrastructures. These vulnerabilities include outdated hardware and software, inadequate security policies and practices, lack of cybersecurity expertise, and inadequate infrastructure. Based on the comprehensive vulnerability assessment, the study recommends the implementation of policies and programs related to information, technology, institutional policy, human capital, and infrastructure to enhance the institution's cybersecurity posture.*

Keywords: Vulnerability, Cybersecurity, Exposure, Sensitivity, Adaptive Capacity

I. INTRODUCTION

Information and communications technology (ICT) has undergone rapid change, drastically altering how we live [1]. These technologies are increasingly needed for important industrial processes and industry control systems. The secretary of the Cybersecurity and Enabling Technology stated in a message on the National Cybersecurity Plan 2022 of the Department of Information and Communication Technology (DICT) that there are specific groups whose ideology is to overthrow the order of our country and are now using cutting-edge and sophisticated technologies to carry out their plans. There are at least six distinct cybercriminal ecosystems that are active in Europe, North and South America, Africa, and Asia, according to a report from Trend Micro. Cybersecurity has risen to the top of the political agenda as cyberspace becomes an integral part of our society. Governments must devise a strategic response to combat cyberthreats in light of the increasing number of reported incidents, particularly for the protection of critical infrastructure. (CI). One of the major strategic challenges many countries face is producing knowledgeable and competent labor in this rapidly evolving field [2].

The Philippine government has been slow to implement the necessary safeguards and measures in Philippine cyberspace that would allow the general public to carry out their business and further their knowledge online without running the risk of being compromised. The Philippines is the ninths most frequently attacked nation worldwide, according to a recent report by the FBI's Internet Crime Complaint Center (IC3) [3]. Despite this, 60% of Philippine businesses reportedly lack the cybersecurity infrastructure necessary to meet the standards set by the modern digital ecosystem. According to cybersecurity firm Kaspersky Lab, the Philippines recorded 10.6 million malware infections in the three months leading up to June, nearly double the level of the first quarter and more than triple the number of threats from a year earlier. Additionally, it was noted that 11.2% of attacks targeted businesses, while 39.4% targeted Kaspersky Internet Security users at home. Most of these web infections involved reprehensible attempts to hijack computers for cryptocurrency mining and data collection. Data from the Kaspersky Security Network (KSN) revealed that the country moved two places up, ranking second among countries most attacked by web threats within the period from January to December last year. The 2022 global ranking is topped by Mongolia with 51.1 percent of the attacks recorded, followed by the Philippines (49.8 percent), Ukraine (49.6 percent), Greece (49.5 percent), and Belarus (49.1 percent) [4].

According to reports, Anonymous Philippines hacked the Philippine Voter's Database server in March 2016, leaking at least 54 million sensitive data online, including 1.3 million passport numbers of Filipinos working abroad [5]. Attempts at hacking, defacing, and Distributed Denial of Service (DDoS) were made against at least 68 government websites in 2016 [6].

The Philippines has experienced cyber espionage before. A security company with headquarters in Finland reportedly discovered malware in 2016 that was aimed at stealing sensitive data from public and private organizations, according to CNN Philippines. When opened, the malicious software known as Remote Access Trojan (RAT) releases a virus into the victim's computer and begins gathering information to be sent back to the attacker [7]. The Philippine government has taken steps to address the issue of cybercrime, including the establishment of the Department of Information and Communications Technology (DICT) in 2016, which oversees the country's cybersecurity initiatives. The DICT has also launched several cybersecurity programs, including the National Cybersecurity Plan, which aims to strengthen the country's cybersecurity capabilities and prevent cyber-attacks [8]. The Philippine National Police Anti-Cybercrime Group estimates that 869 cybercrime incidents, including hacking, identity theft, online con artists, and child sex exploitation, were reported in 2020. One notable cyber-attack that happened in the Philippines was the 2016 Bangladesh Bank heist, in which $81 million from the bank's account at the Federal Reserve Bank of New York was stolen. [9]

Cybersecurity in Higher Education Institutions

The government passed laws as early as 1965 to protect people's property and privacy, including the Anti-Wire Tapping Act of 1965 and the Electronic Commerce Act of 2000. In recent years, Executive Order No. 189 and Republic Act No. 10844 were signed into law to establish the National Cybersecurity Inter-Agency Committee and the DICT, while the National Privacy Commission and Cybercrime Investigation and Coordination Center were created by the Data Privacy Act of 2012 and CyberCrime Prevention Act of 2012. The mission objectives of the National Cybersecurity Plan 2022, aim to create a secure and resilient information infrastructure by strengthening the critical information infrastructure, securing government information infrastructure, raising business sector awareness about cyber risks, and raising individual user awareness.

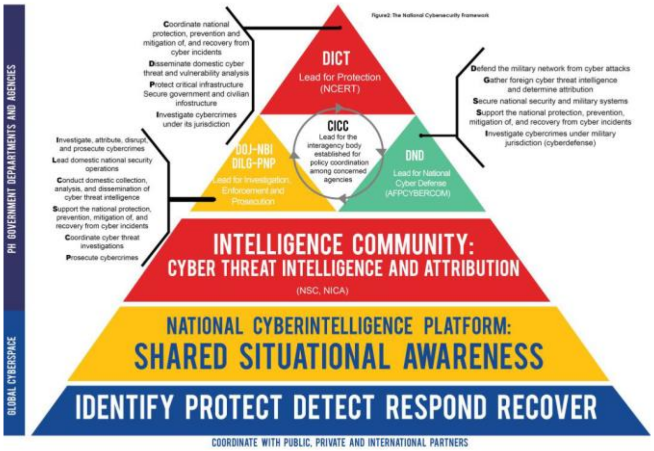

PH GOVERNMENT DEPAARTMENTS AND AGENCIES
GLOBAL CYBERSPACE
Figure2: The National Cybersecurity Framework
Coordinate national protection, prevention and mitigation of, and recovery from cyber incidents
Disseminate domestic cyber threat and vulnerability analysis
Protect critical infrastructure
Secure government and civilian infostructure
Investigate cybercrimes under its jurisdiction
DICT
Lead for Protection (NCERT)
Defend the military network from cyber attacks
Gather foreign cyber threat intelligence and determine attribution
Secure national security and military systems
Support the national protection, prevention, mitigation of, and recovery from cyber incidents
Investigate cybercrimes under military jurisdiction (cyberdefense)
Investigate, attribute, disrupt, and prosecute cybercrimes
Lead domestic national security operations
Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
Support the national protection, prevention, mitigation of, and recovery from cyber incidents
Coordinate cyber threat investigations
Prosecute cybercrimes
DOJ-NBI
DILG-PNP
Lead for Investigation, Enforcement and Prosecution
CICC
Lead for the interagency body established for policy coordination among concerned agencies
DND
Lead for National Cyber Defense (AFPCYBERCOM)
INTELLIGENCE COMMUNITY:
CYBER THREAT INTELLIGENCE AND ATTRIBUTION
(NSC, NICA)
NATIONAL CYBERINTELLIGENCE PLATFORM:
SHARED SITUATIONAL AWARENESS
IDENTIFY PROTECT DETECT RESPOND RECOVER
COORDINATE WITH PUBLIC, PRIVATE AND INTERNATIONAL PARTNERS

Figure 1. The National Cybersecurity Framework of the Philippines (National Strategic Plan 2022, DICT)

The Framework in Figure 1 consists of three layers with different functions, and their activities complement each other to implement the NCSP. The top layer involves exchanging intelligence, the middle layer shares situational awareness, and the bottom layer documents incident responses to inform process improvements [10].

Cyber Threats to Higher Education Institutions

Higher education institutions experience cybersecurity incidents and breaches more frequently, and the sophistication, purpose, and scale of these attacks vary greatly. These range from attempts to interfere with a university network's ability to function to broader and more focused attempts to gather important information from networks and their users. Threats that are sophisticated, persistent, and deliberately aimed at universities are another growing concern because of the sector's significant contribution to innovation and economic growth [11]. Higher education institutions are desirable targets for two reasons. First, colleges and universities house a wide range of sensitive and valuable data, including social security numbers, financial information, medical records, intellectual property, and cutting-edge research. This is similar to what healthcare organizations and financial institutions do. Second, higher education is a particularly vulnerable target for unauthorized access, unsafe Internet use, and malware due to its open-access culture, decentralized departmental or unit-level control, and federated access to data and information [12]. Cybersecurity attacks are also in the news in the Philippines. Unexpected cyber hostilities between China and the Philippines were made public in April 2012. The University of the Philippines was attacked by hackers who claimed to be Chinese. In that case, they altered the UP website (up.edu.ph) by posting a map of the Scarborough Shoal with Chinese characters on it [13]. At a university, cybersecurity often involves more than just safety. The university's network may become interconnected in a spider web-like pattern as a result of the distribution of the list of sensitive data there. When a hacker gains access to one area, they frequently move laterally to other segments to access the desired data [14]. A search on the Privacy Rights Clearinghouse website revealed that from January 2015 to August 2016, hacking or malware-related breaches accounted for 71% of reported breaches at higher education institutions. Due to network vulnerabilities, university-based research, and the accessibility of vast databases of student and employee personal data, threat actors are drawn to an institution's systems. Ransomware and cyberespionage are two threats that are becoming more active in higher education [15]. According to the Commission on Higher Education, 41 cyber incidents were reported in Philippine higher education institutions (HEIs) in 2020. Data breaches, phishing attacks, and website defacement were among the incidents that affected both public and private universities and colleges. The incidents caused sensitive data to be compromised and operations to be disrupted. The National Cybersecurity Plan 2022 emphasizes the need to develop human capabilities across society to effectively prevent cybersecurity risks. This requires a comprehensive approach to education, training, and capacity building that includes both technical and social competencies [16].

SUC: University of Science and Technology of Southern Philippines (USTP)

By virtue of Republic Act 10919, the Mindanao University of Science and Technology (MUST) in Cagayan de Oro City and the Misamis Oriental State College of Agriculture and Technology (MOSCAT) in Claveria, Misamis Oriental merged to establish the University of Science and Technology of Southern Philippines on August 16, 2016. Both campuses are in Northern Mindanao, which is known as the "Gateway to Mindanao," providing a strategic locational advantage for the institution to train and develop students from all over Mindanao. It has maintained its Level IV status as a State University (Highest Distinction) as determined by the Commission on Higher Education (CHED) and the Department of Budget and Management (DBM), and it remains one of the Philippines' 19 leading state universities. The study aims to assess the vulnerability of ICT infrastructures of USTP-CDO and evaluate the effectiveness of the current security practices, policies, and procedures. It also aims to provide recommendations to improve the security posture of USTP-CDO and assess the potential impact of security incidents on its operations and reputation. The study intends to contribute to the research on ICT infrastructure security and provide a reference for other universities and institutions to assess the security of their ICT assets.

II. METHODOLOGY

The study covers the instruction, research and extension, administration, and other support services of the involved sites. The cyber threats experienced by the USTP-CDO are determined, and the resiliency of these ICT infrastructures is evaluated based on assessing their vulnerability. Method of assessment includes the Profiling of ICT infrastructures used by the USTP-CDO, Identification, and Characterization of Cyber threats, Identification of threat exposure and sensitivity, and Development of Exposure Database. The generated vulnerability assessments are the basis for the formulation of policies and other adaptations in the university or colleges. Figure 2 below illustrates the conceptual framework of the study.

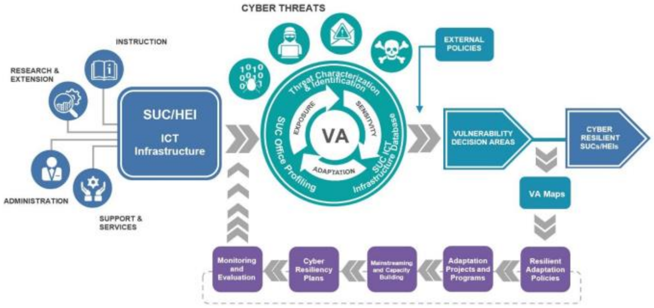
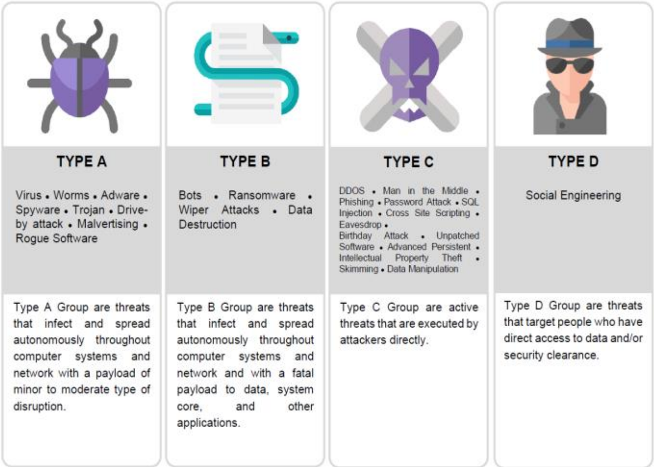

CYBER THREATS
INSTRUCTION
RESEARCH & EXTENSION
ADMINISTRATION
SUPPORT & SERVICES
SUC/HEI
ICT Infrastructure
VA
Threat Characterization & Identification
SENSITIVITY
EXPOSURE
ADAPTATION
SUC Office Profiling
SUC ICT Infrastructure Database
EXTERNAL POLICIES
VULNERABILITY DECISION AREAS
CYBER RESILIENT SUCs/HEIs
VA Maps
Resilient Adaptation Policies
Adaptation Projects and Programs
Mainstreaming and Capacity Building
Cyber Resiliency Plans
Monitoring and Evaluation

Figure 2. Conceptual Framework



TYPE A	TYPE B	TYPE C	TYPE D
Virus • Worms • Adware • Spyware • Trojan • Drive-by attack • Malvertising • Rogue Software	Bots • Ransomware • Wiper Attacks • Data Destruction	DDOS • Man in the Middle • Phishing • Password Attack • SQL Injection • Cross Site Scripting • Eavesdrop • Birthday Attack • Unpatched Software • Advanced Persistent • Intellectual Property Theft • Skimming • Data Manipulation	Social Engineering
Type A Group are threats that infect and spread autonomously throughout computer systems and network with a payload of minor to moderate type of disruption.	Type B Group are threats that infect and spread autonomously throughout computer systems and network and with a fatal payload to data, system core, and other applications.	Type C Group are active threats that are executed by attackers directly.	Type D Group are threats that target people who have direct access to data and/or security clearance.

Figure 3. Threat Identification and Characterization

Development of ICT Infrastructure Exposure Database

The exposure database as shown in Figure 4 was developed by assessing the infrastructure data from every SUC by filling up the Department Profiling Form or ICT Profile Sheet as the research instrument for this study. The form covers both the physical and cyber threat which composes of the main dimensions which consist of data, hardware, software, peopleware, security, environmental factors, and adaptive capacity.

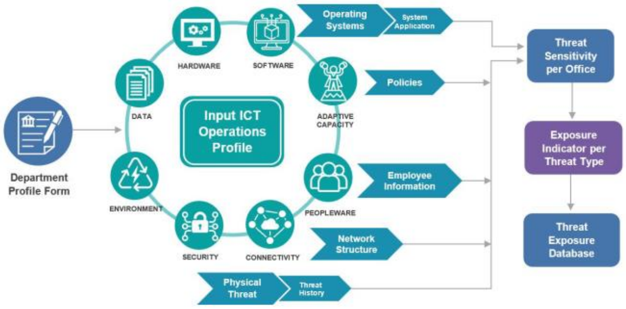


Figure 4. Steps in Developing the ICT Infrastructure exposure database

The main form constitutes some other additional sub-forms that contain additional information corresponding to the overall information system. The form consists of eight (8) sub-forms. Form 1 (Department Profile Form) was used to collect general information about the ICT infrastructures of the buildings which are Data, Hardware, Software, Peopleware, Security, and Environmental factors. The form also covers both the physical and cyber aspects of the building. Form 3. A (Network Structure) indicates network setup in the office. The form was used to collect the hardware devices connected to a certain network whether it is an integrated or isolated network. Form 4. An (Operating System) is used to collect the Operating System utilized by the office while Form 4. B (System Application) is used to collect System Applications. Form 5.A (Employee Information) is used for collecting Employee Information in the office. Form 6.A (Physical Threat) and Form 6. B (Threat History) is used to collect information on reported Physical or Internal Threat incidents that takes place in the office. Form 8.A (Policies) is a set of mitigation options that can be applied to the adaptation of cyber threats based on the technical findings gathered after the assessment. The forms were validated by experts from the Department of Information and Communications Technology and the Institute of Computer Science of the University of the Philippines-Los Baños. They were to examine the questionnaire items for clarity and suitability for use in collecting data for the study. The observations and suggestions of these experts improved the instrument.

Exposure Scoring Indicators

Exposure indicators were considered according to the definition or behavior of the threat. Each threat targets, utilizes, exploits, and attacks certain ICT elements or components such as data files, hardware, software, and peopleware. These components are set in the exposure table in which the ICT profile database is cross-referenced to get the percentage of exposed elements. The different elements are then averaged to get the overall exposure level of the particular office and applied the same process to all offices and for each type of threat type. The overall exposure can be defined as:

$$Overall\ Exposure = \frac{1}{n}\sum_{i=1}^{n} E_i \qquad \text{(Equation 1)}$$

The Overall Exposure can be denoted as:

$$Exposure\ (E_1, E_2, \ldots, E_n) = \frac{E_1 +\ E_2 + \cdots + E_n}{n}$$

where E = the ICT components exposed to certain types of threat, i.e. Data, Hardware, Software, and Peopleware, and n = the total number of ICT components. The percentage of exposed elements is rated in order to get the exposure level using the score table as shown below in Table 1-4.

Table 1. Exposure Score Table for Type A Threat

ICT Components	Exposure Rating				
	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Data Percentage of data types affected by "TYPE A" from the total of data being processed by the corresponding office.	Between 1% to 5%	Between 6% to 10%	Between 11% to 50%	Between 51% to 75%	Between 76% to 100%
Hardware Percentage of hardware affected by a "TYPE A" from the total hardware used by the corresponding office.	Between 1% to 4%	Between 5% to 9%	Between 10% to 50%	Between 51% to 75%	Between 76% to 100%
Software Percentage of software affected by a "TYPE A" from the total software used by the corresponding office.	Less than 1%	Between 1% to 15%	Between 16% to 30%	Between 31% to 60%	Between 61% to 100%
Personnel Percentage of personnel affected by a "TYPE A" from the total number of personnel in the corresponding office.	Less than 1%	Between 1% to 25%	Between 26% to 50%	Between 51% to 75%	Between 76% to 100%

Table 2. Exposure Score Table for Type B Threat

ICT Components	Exposure Rating				
	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Data Percentage of data types affected by "TYPE B" from the total of data being processed by the corresponding office.	Between 0% to 5%	Between 6% to 10%	Between 11% to 50%	Between 51% to 75%	Between 76% to 100%
Hardware Percentage of hardware affected by a "TYPE B" from the total hardware used by the corresponding office.	Between 0% to 4%	Between 5% to 9%	Between 10% to 50%	Between 51% to 75%	Between 76% to 100%
Software Percentage of software affected by a "TYPE B" from the total software used by the corresponding office.	0%	Between 1% to 15%	Between 16% to 30%	Between 31% to 60%	Between 61% to 100%
Personnel Percentage of personnel affected by a "TYPE B" from the total number of personnel in the corresponding office.	0%	Between 1% to 25%	Between 26% to 50%	Between 51% to 75%	Between 76% to 100%

Table 3. Exposure Score Table for Type C Threat

ICT Components	Exposure Rating				
	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Data Percentage of data types affected by "TYPE C" from the total of data being processed by the corresponding office.	Between 0% to 5%	Between 6% to 10%	Between 11% to 50%	Between 51% to 75%	Between 76% to 100%
Hardware Percentage of hardware affected by a "TYPE C" from the total hardware used by the corresponding office.	Between 0% to 4%	Between 5% to 9%	Between 10% to 50%	Between 51% to 75%	Between 76% to 100%
Software Percentage of software affected by a "TYPE C" from the total software used by the corresponding office.	0%	Between 1% to 15%	Between 16% to 30%	Between 31% to 60%	Between 61% to 100%
Personnel Percentage of personnel affected by a "TYPE C" from the total number of personnel in the corresponding office.	0%	Between 1% to 25%	Between 26% to 50%	Between 51% to 75%	Between 76% to 100%

Table 4. Exposure Score Table for Type D Threat

ICT Components	Exposure Rating				
	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Data Percentage of data types affected by "TYPE D" from the total of data being processed by the corresponding office.	Between 0% to 5%	Between 6% to 10%	Between 11% to 50%	Between 51% to 75%	Between 76% to 100%
Hardware Percentage of hardware affected by a "TYPE D" from the total hardware used by the corresponding office.	Between 0% to 4%	Between 5% to 9%	Between 10% to 50%	Between 51% to 75%	Between 76% to 100%
Software Percentage of software affected by a "TYPE D" from the total software used by the corresponding office.	0%	Between 1% to 15%	Between 16% to 30%	Between 31% to 60%	Between 61% to 100%
Personnel Percentage of personnel affected by a "TYPE D" from the total number of personnel in the corresponding office.	0%	Between 1% to 25%	Between 26% to 50%	Between 51% to 75%	Between 76% to 100%

Sensitivity Scoring Indicators

Sensitivity pertains to the degree to which the exposed elements are adversely affected by the corresponding threat. Similarly, sensitivity indicators are considered according to the definition or behavior of the threat. Components and attributes of the ICT infrastructure are the contributing factors for sensitivity. These components are server types, workstations, network accessibility, peripheral devices, operating system, software type, licenses, and technical knowledge of personnel. These components are set in the sensitivity indicator table in which the ICT profile database is then cross-referenced to get the sensitivity score. The threat level of the ICT infrastructure is then rated according to its sensitivity score using the score table shown as shown in Equation 2. The average score is computed to get the overall threat level for each particular office and for each type of threat. The overall sensitivity can be defined as:

$$Overall\ Sensitivity = \frac{1}{n}\sum_{i=1}^{n} S_i \qquad \text{(Equation 2)}$$

The Overall Sensitivity can be denoted as:

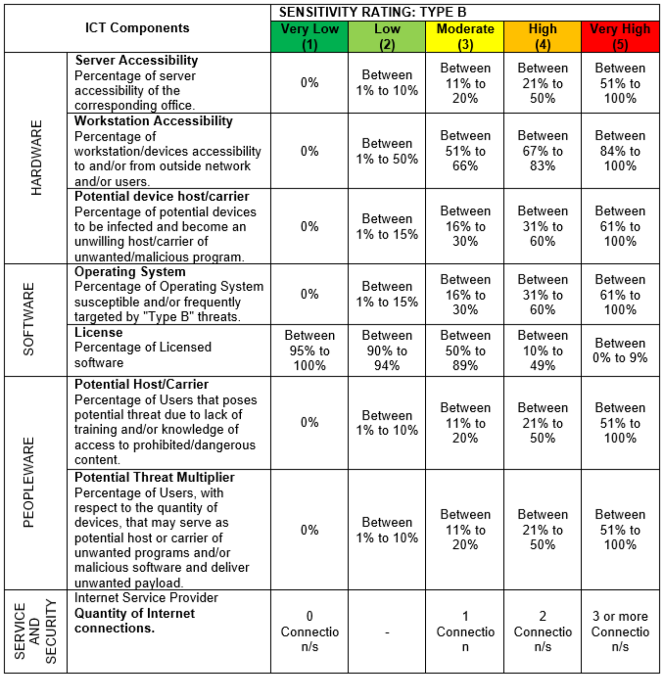
$$Sensitivity\ (S_1, S_2, \ldots, S_n) = \frac{S_1 +\ S_2 + \cdots + S_n}{n}$$

where S = the ICT components and contributing factor for sensitivity, i.e. Sever Accessibility, Workstation Accessibility, Potential device host/carrier, Operating System, and License, and n = the total number of ICT components. The percentage of sensitivity elements is rated in order to get the sensitivity level using the score table as shown below in Table 5-8.

Table 5. Sensitivity Score Table for Type A Threat

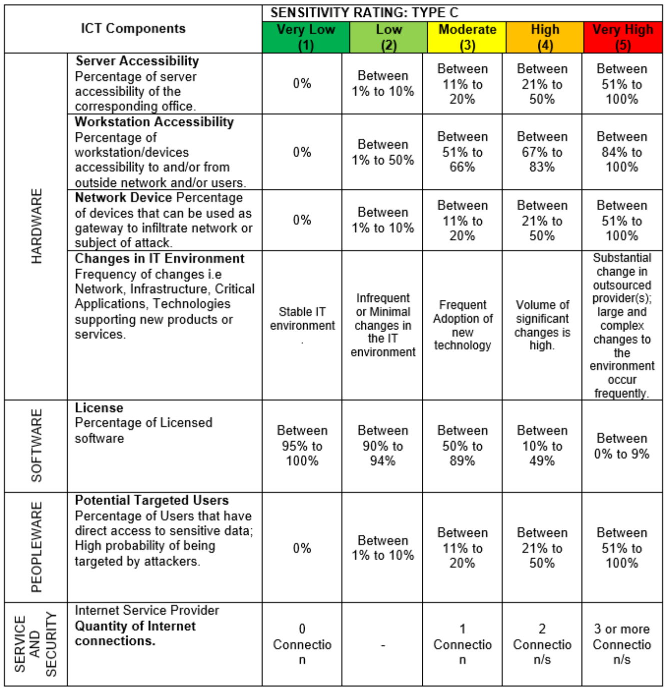
ICT Components		SENSITIVITY RATING: TYPE A				
		Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
SOFTWARE	**Operating System** Percentage of Operating System susceptible and/or frequently targeted by "Type A" threats.	Less than 1%	Between 1% to 15%	Between 16% to 30%	Between 31% to 60%	Between 61% to 100%
	License Percentage of Licensed software	Between 95% to 100%	Between 90% to 94%	Between 50% to 89%	Between 10% to 49%	Between 0% to 9%
PEOPLEWARE	**Potential Host/Carrier** Percentage of Users that poses potential threat due to lack of training and/or knowledge of access to prohibited/dangerous content.	Less than 1%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
	Potential Threat Multiplier Percentage of Users, with respect to the quantity of devices, that may serve as potential host or carrier of unwanted programs and/or malicious software and deliver unwanted payload.	Less than 1%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
SERVICE AND SECURITY	**Internet Service Provider** Quantity of Internet connections.	0 Connection/s	-	1 Connection	2 Connection/s	3 or more Connection/s

Table 6. Sensitivity Score Table for Type B Threat



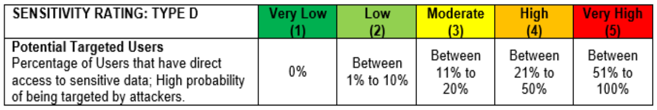
	ICT Components	SENSITIVITY RATING: TYPE B				
		Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
HARDWARE	**Server Accessibility** Percentage of server accessibility of the corresponding office.	0%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
	Workstation Accessibility Percentage of workstation/devices accessibility to and/or from outside network and/or users.	0%	Between 1% to 50%	Between 51% to 66%	Between 67% to 83%	Between 84% to 100%
	Potential device host/carrier Percentage of potential devices to be infected and become an unwilling host/carrier of unwanted/malicious program.	0%	Between 1% to 15%	Between 16% to 30%	Between 31% to 60%	Between 61% to 100%
SOFTWARE	**Operating System** Percentage of Operating System susceptible and/or frequently targeted by "Type B" threats.	0%	Between 1% to 15%	Between 16% to 30%	Between 31% to 60%	Between 61% to 100%
	License Percentage of Licensed software	Between 95% to 100%	Between 90% to 94%	Between 50% to 89%	Between 10% to 49%	Between 0% to 9%
PEOPLEWARE	**Potential Host/Carrier** Percentage of Users that poses potential threat due to lack of training and/or knowledge of access to prohibited/dangerous content.	0%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
	Potential Threat Multiplier Percentage of Users, with respect to the quantity of devices, that may serve as potential host or carrier of unwanted programs and/or malicious software and deliver unwanted payload.	0%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
SERVICE AND SECURITY	Internet Service Provider **Quantity of Internet connections.**	0 Connectio n/s	-	1 Connectio n	2 Connectio n/s	3 or more Connectio n/s

Table 7. Sensitivity Score Table for Type C Threat



	ICT Components	SENSITIVITY RATING: TYPE C				
		Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
HARDWARE	**Server Accessibility** Percentage of server accessibility of the corresponding office.	0%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
	Workstation Accessibility Percentage of workstation/devices accessibility to and/or from outside network and/or users.	0%	Between 1% to 50%	Between 51% to 66%	Between 67% to 83%	Between 84% to 100%
	Network Device Percentage of devices that can be used as gateway to infiltrate network or subject of attack.	0%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
	Changes in IT Environment Frequency of changes i.e Network, Infrastructure, Critical Applications, Technologies supporting new products or services.	Stable IT environment .	Infrequent or Minimal changes in the IT environment	Frequent Adoption of new technology	Volume of significant changes is high.	Substantial change in outsourced provider(s); large and complex changes to the environment occur frequently.
SOFTWARE	**License** Percentage of Licensed software	Between 95% to 100%	Between 90% to 94%	Between 50% to 89%	Between 10% to 49%	Between 0% to 9%
PEOPLEWARE	**Potential Targeted Users** Percentage of Users that have direct access to sensitive data; High probability of being targeted by attackers.	0%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%
SERVICE AND SECURITY	Internet Service Provider **Quantity of Internet connections.**	0 Connectio n	-	1 Connectio n	2 Connectio n/s	3 or more Connectio n/s

Table 8. Sensitivity Score Table for Type D Threat



SENSITIVITY RATING: TYPE D	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Potential Targeted Users Percentage of Users that have direct access to sensitive data; High probability of being targeted by attackers.	0%	Between 1% to 10%	Between 11% to 20%	Between 21% to 50%	Between 51% to 100%

Adaptive Capacity Scoring Indicators

The Adaptive Capacity pertains to the ability of the SUC to adjust to threats or respond to consequences. The indicators include technology, information, infrastructure, policies, human capital, and wealth. The indicators derived from the profile database and supported by the university policy are scored accordingly using the score table as shown below and computed to get the overall adaptive capacity level. Depending on the administrative structure, the adaptive capacity level can be treated per department separately or as a single rating for the whole SUC. The overall adaptive capacity can be defined as:

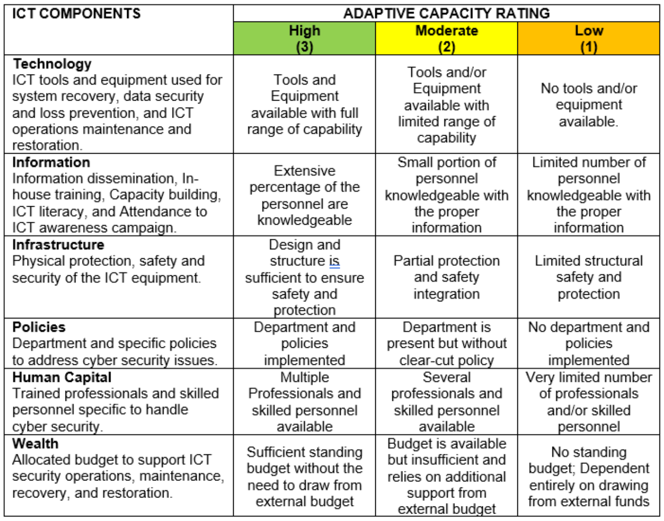
$$Overall\ Adaptive\ Capacity = \frac{1}{n}\sum_{i=1}^{n} C_i \qquad \text{(Equation 3)}$$

The Overall Adaptive Capacity can be denoted as:

$$Adaptive\ Capacity\ (C_1, C_2, \ldots, C_n) = \frac{C_1 + C_2 + \cdots + C_n}{n}$$

where C = the Adaptive Capacity Components, i.e. Technology, Information, Infrastructure, Policies, Human Capital, and Wealth, and n = the total number of Adaptive Components shown in Table 9. Depending on the administrative structure, the adaptive capacity level can be treated per department separately or as a single rating for the whole SUC.

Table 9. Adaptive Capacity Score Table



ICT COMPONENTS	ADAPTIVE CAPACITY RATING		
	High (3)	Moderate (2)	Low (1)
Technology ICT tools and equipment used for system recovery, data security and loss prevention, and ICT operations maintenance and restoration.	Tools and Equipment available with full range of capability	Tools and/or Equipment available with limited range of capability	No tools and/or equipment available.
Information Information dissemination, In-house training, Capacity building, ICT literacy, and Attendance to ICT awareness campaign.	Extensive percentage of the personnel are knowledgeable	Small portion of personnel knowledgeable with the proper information	Limited number of personnel knowledgeable with the proper information
Infrastructure Physical protection, safety and security of the ICT equipment.	Design and structure is sufficient to ensure safety and protection	Partial protection and safety integration	Limited structural safety and protection
Policies Department and specific policies to address cyber security issues.	Department and policies implemented	Department is present but without clear-cut policy	No department and policies implemented
Human Capital Trained professionals and skilled personnel specific to handle cyber security.	Multiple Professionals and skilled personnel available	Several professionals and skilled personnel available	Very limited number of professionals and/or skilled personnel
Wealth Allocated budget to support ICT security operations, maintenance, recovery, and restoration.	Sufficient standing budget without the need to draw from external budget	Budget is available but insufficient and relies on additional support from external budget	No standing budget; Dependent entirely on drawing from external funds

Vulnerability Assessment

The process of determining vulnerabilities along with their associated risks is called vulnerability assessment [17]. Vulnerability assessment is considered a proactive defensive methodology as it plays a significant role in protecting computer systems, applications, and network infrastructures. Vulnerabilities in different operating systems and applications could lead to essential security violations and exploits. Security breaches increased the potential for system compromise, data loss, and exposure of sensitive information [17].

In this paper, we conduct a vulnerability assessment of the ICT infrastructures in the buildings of Cagayan State University which can be affected by the 4 main cyber threat categories. In order to get the vulnerability index of the buildings in the university, there was an intersection of the computed score on the exposure and sensitivity over the computed score on the adaptive capacity for each building. The vulnerability index is computed using the following formula:

$$VI = \frac{Exposure\ x\ Sensitivity}{Adaptive\ Capacity} \qquad \text{(Equation 4)}$$

Where, VI = the vulnerability index of the buildings, Exposure = computed average scores of the exposure indicators, Sensitivity = computed average scores of the sensitivity indicators, and Adaptive Capacity = computed average scores of the adaptive capacity indicators. A five-point rating scale is also generated to assess the vulnerability of each infrastructure. This five-point scale is presented in Table 10.

Table 10. A five-point rating scale for vulnerability assessment.

Vulnerability Index	Vulnerability Category	Color
< 1	Very Low	🟩
1 to 2	Low	🟩
> 2 to 4	Moderate	🟨
> 4 to 10	High	🟧
> 10	Very High	🟥

III. RESULTS AND DISCUSSIONS

Summary of USTP-CDO ICT Infrastructures

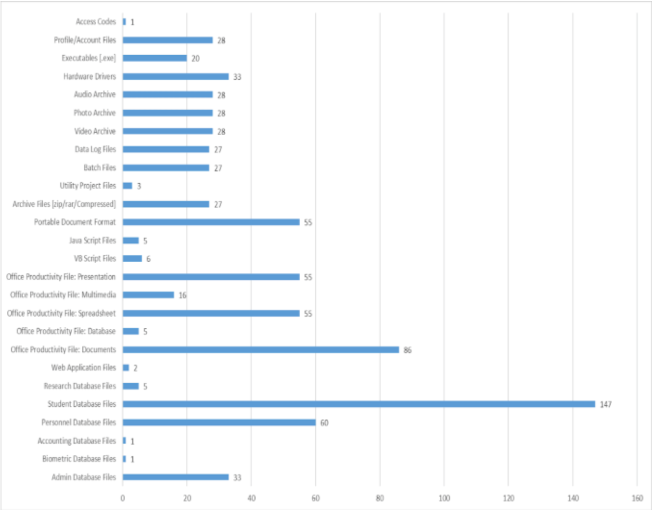


Figure 5. Data file types utilized by offices in USTP-CDO

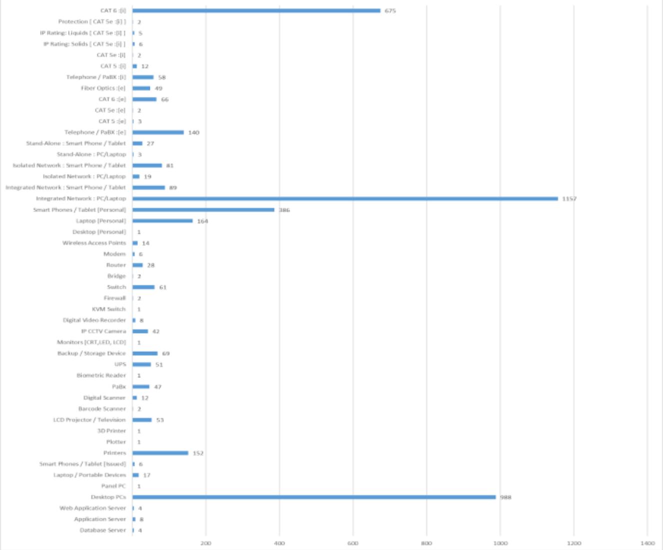


Figure 6. Hardware components used USTP-CDO

In Figure 5, the university holds student information which is in the Student Database Files. The university uses an Integrated School Management Solution (PRISMS) which includes an enrolment system, class schedule, student information system, mobile application, and queuing information system. Even the library management information system is a facility that uses student information aside from books and resources management for library services. Office productivity tools are next in line with the most utilizes data in the offices. In Figure 6, the university utilized a fiber-optic backbone to interconnect buildings to the data center, while all computer is connected to the different network using CAT6. Almost 1,157 computers/laptops are connected to either wired or wireless networks in the university. These are laboratories, libraries, and offices using desktop PCs.

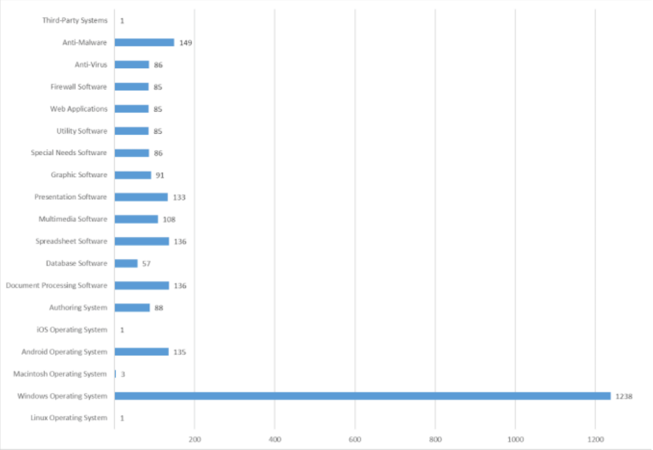


Figure 7. Software utilized by USTP-CDO

Figure 7, shows that the university subscribes to a licensed operating system, the MSDN for laboratories while for individual licenses (OEM) for offices and special laboratories. The productivity software/tools are licensed under MSDN and OEM for key offices using MS Offices. For anti-malware, the university uses Windows Defender and Sophos endpoint anti-virus. The network is also protected by a firewall security appliance (UTM: universal threat management), Sophos with end-point anti-virus to protect end-point users.

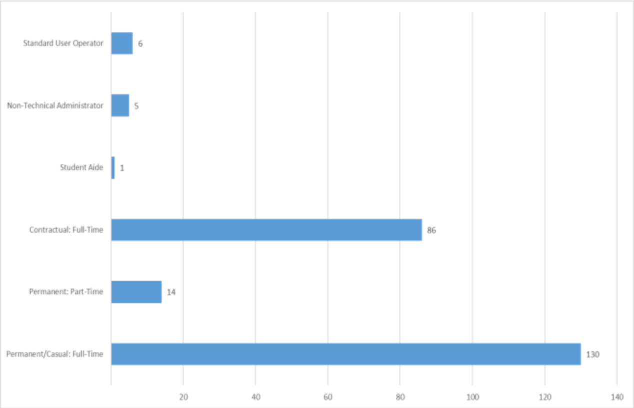


Figure 8. Personnel info in USTP-CDO

In Figure 8, the university has (287) full-time and (139) part-time faculty while there are (64) full-time and (236) job order personnel. During the inventory, only warm bodies were accounted for during the working hour period. Most faculty have their personal laptop and smartphones. Frontlines like deans, program chairs, and service offices are provided with desktop PCs and are connected to the university network. Ground personnel have their personal gadgets connected to the network through wireless connectivity upon registration of their device to the ICT office.

The Vulnerability Assessment of USTP

Type A Threat shows that 33 offices (38%) from the University of Science and Technology of Southern Philippines have Very High Exposure, and 53 offices have High Exposure to Type A Threats. This means that the Data, Hardware, and Software for those specific offices have low susceptibility to Type A threats which include viruses, worms, Trojans, adware, etc. The table also shows that 72 offices (84%) have Low Sensitivity to Type A threats. It can also be observed that all the offices have Very High Adaptive Capacity. This results in 72 of the offices (84%) having Low Vulnerability while only 14 offices (16%) have Moderate Vulnerability to Type A threats.

Type B Threat shows that 65 offices (76%) from the university have High Exposure while 19 offices (22%) have Very High Exposure to Type B Threats. This means that the Data, Hardware, and Software for those specific offices have low susceptibility to Type B threats which include bots, ransomware, wiper attacks, and data destruction. The table also shows that most of the offices (84%) have Low Sensitivity to Type B threats. It can also be observed that most of the offices (98%) have Moderate Adaptive Capacity. This resulted in 78 of the offices (91%) having Moderate Vulnerability, 5 offices (6%), and 3 offices (3%) having High and Low Vulnerabilities to Type B threats respectively.

Type C Threat shows that most of the offices (63%) from the University have Moderate Exposure to Type C Threats. This means that the Data, Hardware, and Software have high susceptibility to Type C threats like denial-of-service (DDoS), man in the middle, phishing, password attack, intellectual property theft, etc. It can also be observed that most of the offices (88%) have Low Sensitivity while most of the offices (98%) have Moderate Adaptive Capacity to Type C threats. This results in 60 (70%) of the offices having Low Vulnerability and 26 offices (30%) having Moderate Vulnerability to this kind of threat.

Type D Threat shows that almost all offices (93%) from USTP have Very Low Exposure and Very Low Sensitivity to Type D Threats. This means that the personnel in these offices have a very low percentage of exposure to Social Engineering attacks. Only 5 (6%) of the offices have Very High Exposure and Sensitivity to Type D Threats. It can also be observed that almost all offices (98%) have Very High Adaptive Capacity. This results in 80 offices (93%) which have a Very Low Vulnerability while five offices (6%) have a High Vulnerability and only one office has a Moderate Vulnerability to Type D threat.

CONCLUSIONS

Based on the comprehensive vulnerability assessment, the study recommends mitigation policies in the areas of information, technology, institutional policy, human capital, and infrastructure. The policies include producing IEC materials, conducting regular cybersecurity fora, capacity building programs, centralizing databases in a secured data center, replacing outdated workstations, conducting regular audits of protocols and practices, and establishing an in-house security team to manage security policies, among others. The implementation of the recommended mitigation policies and programs can help enhance the institution's cybersecurity posture and mitigate the identified vulnerabilities. However, the success of the policies and programs will depend on the institution's commitment to prioritize cybersecurity as a critical area of concern. It is necessary to allocate sufficient resources, including finances, personnel, and time, to implement the policies and programs effectively.

ACKNOWLEDGMENT

The authors would like to express their deep gratitude to Cagayan State University and the Commission on Higher Education, in collaboration with the University of Science and Technology of Southern Philippines, for their generous support and funding, which made this study possible. The authors would also like to extend their sincerest appreciation to the employees of USTP-CDO and ICT Services Personnel for their valuable contributions to the success of the study.

REFERENCES

[1] NCSP2020. (2017). National Cybersecurity Plan 2020. Department of Information and Communication Technology, Cybercrime Investigation and Coordination Center. Quezon City, Philippines: DICT. Retrieved July 18, 2019, from https://dict.gov.ph/wp-content/uploads/2019/07/NCSP2022-rev01Jul2019.pdf

[2] Radunović, V., & Rüfenacht, D. (2016). Cybersecurity Competence Building Trend. DiploFoundation. Msida, Malta: DiploFoundation. Retrieved December 4, 2018,

[3] Mastrangelo, Lindsey. (2023) “2021 Internet Crime Report.” Homeland Security Digital Library, 26 Jan. 2023, https://www.hsdl.org/c/2021-internet-crime-report/

[4] Ronda, R. A. (2023, March 14). ‘Philippines 2nd most attacked by web threats worldwide last year.’ Philstar.com. https://www.philstar.com/headlines/2023/03/15/2251710/philippines-2nd-most-attacked-web-threats-worldwide-last-year https://www.diplomacy.edu/sites/default/files/Cybersecurity%20Full%20Report.pdf

[5] Anonymous Philippines. (2016, March). Philippine Voter's Database Server Hacked; 54 Million Records Leaked Online, including 1.3 Million Passport Numbers of Filipinos Working Abroad [Press release]. Retrieved from https://www.anonops.net/news/philippine-voters-database-server-hacked-54-million-records-leaked-online-including-1-3-million-passport-numbers-of-filipinos-working-abroad/

[6] Mateo, J. (2016, July 16). 68 gov't websites were attacked. Retrieved December 5, 2018, from The Philippine Star:

https://www.philstar.com/headlines/2016/07/16/1603250/68-govt-websites-attacked

[7] Gotinga, J., & Tan, L. (2016, August 5). Suspected Chinese malware used to spy on PH gov't – security firm. Retrieved from CNN Philippines: http://nine.cnnphilippines.com/news/2016/08/05/South-China-Sea-RAT-cyber-attack-Philippines.html

[8] Manila Bulletin. (2020, June 11). DICT rolls out National Cybersecurity Plan. Retrieved April 6, 2023, from https://mb.com.ph/2020/06/11/dict-rolls-out-national-cybersecurity-plan/

[9] Philippine National Police Anti-Cybercrime Group. (2021). Cybercrime Statistics. Retrieved April 6, 2023, from https://acg.pnp.gov.ph/index.php/statistics

[10] Department of Information and Communications Technology (DICT). (n.d.). National Cybersecurity Plan 2022. Retrieved April 6, 2023, from https://dict.gov.ph/national-cybersecurity-plan-2022/

[11] UniversitiesUK. (2013). Cyber security and Universities: Managing the Risk. London, UK: Universities UK. Retrieved November 26, 2018, from https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf

[12] Fishman, T. D., Cole, C., & Grama, J. L. (2018, February 22). Elevating Cybersecurity on the Higher Education Leadership Agenda: Increasing executive fluency and engagement in cyber risk. Retrieved December 4, 2018, from Deloitte Insights: https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

[13] Aurelio, J. M. (2012, April 20). UP site hacked over Scarborough Shoal. Retrieved December 12, 2018, from Inquirer.Net: https://technology.inquirer.net/10063/up-site-hacked-over-scarborough-shoal

[14] Secureworks. (2016). The Surge of Cyber Threats: What Higher Education Needs to Know. Atlanta, USA: SecureWorks. Retrieved from SecureWorks, Inc.

[15] Privacy Rights Clearinghouse. (2016). Higher Education Breach List. Retrieved April 6, 2022, from https://www.privacyrights.org/data-breaches?f%5B0%5D=field_type_of_breach%3A273

[16] CHED. (2021). CHED Cybersecurity Task Force: Annual Report 2020. Retrieved April 6, 2023, from https://ched.gov.ph/ched-cybersecurity-task-force-annual-report-2020/

[17] Akour, M., & Alsmadi, I. (2016). Vulnerability assessments: A case study of Jordanian universities. 2015 International Conference on Open Source Software Computing, OSSCOM 2015. Institute of Electrical and Electronics Engineers Inc.