



CYBERSECURITY IN THE PHILIPPINES: AN ASSESSMENT

Kier Gabriel Tampus, Charles Phillippe O. Garcia

ABSTRACT

Cybersecurity is one of the issues are being confronted here and abroad for it affects the political, economic, and social factors. The various aspects regarding cybersecurity such as awareness, challenges, modernization in the Philippine setting, efficiency and opportunities are the factors to be considered in order to secure the welfare of the people here and abroad. In connection with national security, awareness and proper information dissemination about cybersecurity must be imposed for further understanding on its significance towards society. The different institutions such as the government, mass media and schools are vital pillars towards in-depth comprehension on the awareness, challenges, efficiency and opportunities of cybersecurity and this led to this study. Using the frequency distribution and weighted mean in demographic profile and the survey proper, in that order, plus the narrative answers on the qualitative part of the survey sheet will give the readers a deeper insight and recommendations about cybersecurity in the Philippine setting.

KEYWORDS: *Cybersecurity, Data Privacy, Data Protection, Private-Public Partnership*

INTRODUCTION

Cybersecurity is one of the issues that bring challenges here and abroad for it affects the economic, political, sociological and even psychological aspects of the people. The concept itself refers to things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet (Cambridge Dictionary). This implies that the welfare of the people must be secured at all times to be free from any harm or danger that may be brought either by local or international threats. According to the report of [tradepassglobal.com](https://www.tradepassglobal.com), the shortage of cybersecurity personnel in the Philippines has given rise to outsourcing and the involvement of foreign consultants which is only too expensive and not sustainable to say the least. Therefore, considering the present state of events, upskilling current cybersecurity professionals in the country and also training new ones is the only reliable option. (<https://www.tradepassglobal.com/blogs/why-philippines-needs-to-upskill-current-cybersecurity-professionals-in-the-country/>)

The concept of cybersecurity is connected with the program Bachelor of Science in Criminology (BSC) for its curriculum includes subjects pertaining to security and law enforcement and this gives a connotation that only BS Criminology graduates have the high chance to be employed as cybersecurity experts. In addition, Mapua University offers BS Cybersecurity starting SY 2026-2027 and this gives an opportunity to its future graduate to be employed in a lucrative job. The addition of the BS Cybersecurity program in Mapua University's curricular offerings can be considered as an additional means to disseminate information about cybersecurity since the said university is considered as center of excellence in engineering ([see https://www.facebook.com/share/p/14SvsGbALNQ/](https://www.facebook.com/share/p/14SvsGbALNQ/))

According to cybersecurityguide.org, the commo job titles related to cybersecurity are as follows: Cybersecurity Specialists, Information Security Specialists, Security Specialists, Cybersecurity Analysts and Privacy Specialists with the qualifications: Education, Industry certifications and clearances, Experience, and Network. In addition, according

to <https://www.ziprecruiter.com/>, to be employed as a cybersecurity professional, he or she must acquire relevant skills through courses in network security, programming, and systems administration. Earning certifications such as CompTIA Security+ or CISSP can improve job prospects, and gaining hands-on experience through internships or labs is highly valuable.

One of the key highlights of the report of <https://gamma.app/> is that per industry report, cybercrimes incident had an 4,469 cases or an increase of 21.84% in 2024 compared with that of 3,668 of 2023 and this lead need the demand for cybersecurity due to big possible backlog of cybersecurity cases.

The <https://cybercrime.gov.in/> gave three (3) ways to prevent cybercrime and this includes: 1) Cyber awareness and hygiene for parents; 2) Cyber awareness and hygiene for teens and young adults; and 3) Cyber awareness and hygiene for organizations

Based on the article of www.aibp.sg. The Philippines faces one of the most severe cybersecurity talent shortages in the region, leaving businesses and government agencies vulnerable to attacks. Without a strong cybersecurity workforce, the country's ability to defend critical infrastructure, financial institutions, and digital services remains at risk. In addition, as digital transformation accelerates across ASEAN, the shortage of cybersecurity professionals has become a significant barrier to securing businesses and government systems. The Philippines is among the hardest-hit countries, with organizations struggling to find qualified cybersecurity talent to defend against rising cyber threats. (<https://www.aibp.sg/articles/strengthening-cybersecurity-in-the-philippines>)

Based on the May 4, 2025 article of Business World entitled Philippines struggles to keep cyberwarriors due to tech brain drain and one of the examples is Jericho P. Dupo, a 25-year-old full-stack developer at IBM Philippines, is looking for a job overseas, where he expects to earn more and gain more experience as a cybersecurity expert.

For him benefits, experiences and social networks that he can have access to once he started working overseas will be



much greater,” said the Filipino cyberwarrior, whose job involves patching up web-based software from threats and vulnerabilities. He also uttered that the the pay in Manila is too low despite the high cost of living.

In addition, eight (8) of 10 Filipino cyber-experts work overseas, and there are only 200 of them remaining compared with 2,000 in Singapore, former Information and Communications Technology Secretary Ivan John E. Uy has said.

<https://wealthinsights.metrobank.com.ph/bworldonline/philippines-struggles-to-keep-cyberwarriors-due-to-tech-brain-drain>

The awareness, challenges, modernization, efficiency, opportunities about cybersecurity will serve as the concerns to be addressed in this study plus the points of view of the respondents on how can the government address the aforementioned issues.

Statement of the Problem

This study focused on Cybersecurity in the Philippines: An Assessment

Specifically, it sought to answer the following problems:

1. What is the profile of the respondents in terms of the following factors:
 - 1.1 age;
 - 1.2 sex;
 - 1.3 highest educational attainment; and
 - 1.4 length of employment
2. What is the degree of agreement of the respondents on the awareness on cybersecurity in the Philippines as to:
 - 2.1 high chance of employment;
 - 2.2 the job is for graduates of BS Criminology only;
 - 2.3 the IT-related courses graduates on cybersecurity works; and
 - 2.4 the general public's awareness about employment connected to cybersecurity
3. What is level of agreement of the respondents on the challenges of cybersecurity in the Philippines in relation with:
 - 3.1 limitations of employment opportunities;
 - 3.2 employment rate abroad;
 - 3.3 strict qualifications for employment;
 - 3.4 internet connection on the delivery of the works of cybersecurity experts;
 - 3.5 policies and programs about cybersecurity; and
 - 3.6 trainings/certifications for cybersecurity
4. What is the perceived agreement of the respondents on the modernization of cybersecurity in the Philippines particularly in:
 - 4.1 backlog in the data regarding cybersecurity issues;
 - 4.2 upgrade in technology; and
 - 4.3 Filipino-owned internet provider
5. What is the extent of agreement of the respondents on the efficiency of cybersecurity in the Philippines in connection with:
 - 5.1 solving cybercrime-related cases; and
 - 5.2 training of Filipino cybersecurity experts abroad
6. For the respondents, what is the presumed agreement on the opportunities in cybersecurity in the Philippines particularly about:

6.1 non-BS Criminology graduates as cybersecurity expert; and

6.2 on hiring cybersecurity experts

7. What is the stance of the respondents on the policies or programs the Philippine government must impose regarding cybersecurity?

METHODOLOGY

Research Design

This study utilized quantitative research through survey methods or use of a researcher-made questionnaire. Research methods refer to the systematic approaches and techniques employed to gather, analyze, interpret, and draw conclusions from data in a structured and rigorous manner. The researcher adequately constructed a survey questionnaire-checklist sufficient to gather the needed data to complete the study. In addition, the last part of the survey sheet is a qualitative portion where the respondents will give an answer in 2-3 sentences only.

Through survey technique, the researcher used the research instrument that was validated by experts and later on assessed with reliability statistics to assure the internal consistency of the items. Once reliable, the data were gathered through the research instrument that was floated or sent to the respondents both via online or through Google Forms and face-to-face administration of the instrument after the researcher made appointments to the qualified respondents. The final data were simplified in a matrix for systematic data analysis.

Population of the Study

A total of 30 samples served as the final respondents of the study. The samples were taken from various sectors/units that are connected with cybersecurity yet the details of their office/deployment will not be divulged due to confidentiality of their profile and their office.

Data Gathering Tool

The researcher used a two-part survey sheet where the first part focused on the demographic profile of the respondents particularly on age, sex, highest educational attainment and length of employment. On the other hand, the second part deals with scenarios that centered on the awareness of the public awareness on employment, challenges, modernization, efficiency and opportunities of cybersecurity in the Philippines. Lastly, the qualitative part of the tool sought the insight of the respondents on the policies or programs the Philippine government must impose to strengthen the awareness and efficiency of cybersecurity.

For the first part or the demographic profile, the respondents have options where they will tick mark the most appropriate answer. On the other hand, for the second part, it used a Likert Scale with the numerical options 1,2,3,4, and 5 with a corresponding descriptive mark of Strongly Disagree (DA), Disagree (DA), Moderately Agree (MA), Agree (A) and Strongly Agree (SA), in that order.

Data Gathering Procedure

The procedure in data gathering commenced from the time the research instrument was fully assessed of its validity and reliability. From thereon onwards, the researcher sent



communication letters or notices, both printed in black and white and email to all the participants since others might not participate in the study. The respondents that gave their consent on the study, or replied with the communication sent to them were either sent with a questionnaire in Google forms, or visited by the researcher for personal administration of the research instrument. Hence, the survey instrument was floated or administered to the respondents both in person and through online means.

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

The complete data of the study were simplified in a matrix, where all the data from the sample respondents need to be placed. Incomplete data or responses coming from any

respondent were disregarded since they affected the integrity of the whole study or the missing data were substantial. The responses made through online means were gathered by downloading the responses and extracting them carefully to be included in the paper-based results, in the matrix earlier prepared to maintain the integrity and accuracy of the data. The researcher gathered the data from the respondents within a 45-day period. Thereafter, the simplified data were attained, computations and analysis that aided the researcher in interpreting the results and made inferences.

Treatment of the Data

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

Frequency Count and Percentage is used in the descriptive measurement of data in the profile of the respondents such as age, sex, highest educational attainment and length of employment.

Weighted Mean or Average is used in measuring the agreement of the respondents on the awareness on employment, challenges, modernization, efficiency and opportunities of cybersecurity in the Philippines.

RESULTS AND DISCUSSION

Sex	Frequency	Percentage	Rank
Male	22	73.33	1
Female	8	26.67	2
Total	30	100	

Table 1. Respondents' Sex

Table 1 shows that 22 or 73.33% of the respondents were male while the remaining eight (8) or 26.67% were female.

It can be deduced that most of the respondents were male.

Age	Frequency	Percentage	Rank
21-25	12	40.00	1
26-30	7	23.33	3
31-35	1	3.33	4
36-ABOVE	10	33.33	2
Total	30	100	

Table 2. Respondents' Age

Table 2 emphasizes that 12 or 40% aged 21-25 years old, 10 or 33.33% were 36 years old and above, seven (7) or 23.33% were between 26-30 years old and one (1) or 3.33% is between 31-35 years old.

It can be inferred that most of the respondents were in between 21-25 years old.

Civil Status	Frequency	Percentage	Rank
Single	25	83.33	1
Married	5	16.67	2
Separated	0	0.00	3.5
Widow/Widower	0	0.00	3.5
Total	30	100	

Table 3. Respondents' Civil Status

The third table presented that 25 or 83.33% of the respondents were single while five (5) or 16.67% were married. None of them were separated nor widow/widower.

It can be implied that most of the respondents were single.



Highest Educational Attainment	Frequency	Percentage	Rank
Baccalaureate	21	70.00	1
Master's (Units)	1	3.33	4
Master's Degree	6	20.00	2
Doctorate (Units)	0	0.00	5
Doctorate Degree	2	6.67	3
Total	30	100	

Table 4. Respondents' Highest Educational Attainment

The respondents' highest educational attainment was shown at the fourth table where it says that 21 or 70% attained baccalaureate degree; six (6) or 20% have finished master's degree; two (2) or 6.67% obtained doctorate degree; one (1) or

3.33% had units in master's program and none had units in doctorate degree.

It can be construed that most of the respondents finished baccalaureate degree.

Length of Employment (in years)	Frequency	Percentage	Rank
less than a year	13	43.33	1
2-5	6	20.00	3
6-10	2	6.67	4
11- above	9	30.00	2
Total	30	100	

Table 5. Respondents' Length of Employment

The 5th table revealed that 13 or 43.33% of the respondents were employed for less than a year; nine (9) or 30% were stayed for 11 years and above; six (6) or 20% were employed for 2-5 years and two (2) or 6.67% for 6-10 years.

It can be presumed that most of the respondents were employed for less than a year.

Question Number	Description	Weighted Mean	Descriptive Remarks
A.1	Cybersecurity is known in the Philippines because of the high chance of employment or being employed.	2.47	Disagree
A.2	The job related to cybersecurity is for the graduates of BS Criminology only.	2.28	Disagree
A.3	Information Technology-related course graduates can be employed as cybersecurity experts.	3.80	Agree
A.4	The general public is aware on the existence of jobs related to cybersecurity.	2.37	Disagree

Table 6. On the Awareness on Cybersecurity in the Philippines

It can be gleaned at the 6th table that questions A.3 had a weighted mean of **3.80** (Agree) while the remaining questions A.1, A.2 and A.4 got a weighted mean of 2.47, 2.28 and 2.37, in that order, a descriptive remarks of Disagree.

It can be deduced that most of the respondents were disagree on the awareness of the people about cybersecurity in the Philippines.

Question Number	Description	Weighted Mean	Descriptive Remarks
B.1	The employment opportunities for cybersecurity in the Philippines is very limited.	3.57	Agree
B.2	The employment rate for cybersecurity abroad is high or very high.	4.07	Agree
B.3	Strict qualifications for cybersecurity reduce employment opportunities	3.63	Agree
B.4	The slow internet speed in the country affects the performance of the cybersecurity experts.	4.03	Agree
B.5	The government has limited if none programs and policies towards cybersecurity expert.	3.62	Agree
B.6	The training programs/certifications for cybersecurity expert is limited.	3.67	Agree

Table 7. On the Challenges of Cybersecurity in the Philippines



Presented in the 7th table that all of the six (6) scenarios had a descriptive remarks of Agree.

It can be inferred that most of the respondents agreed on the challenges of cybersecurity in terms of employment, trainings and programs.

Question Number	Description	Weighted Mean	Descriptive Remarks
C.1	The backlog in the data regarding cybersecurity issues is challenging to be addressed.	3.63	Agree
C.2	The low-technology in the country is needed to be upgraded to support cybersecurity.	4.07	Agree
C.3	The modernization of internet in the country must be delegated to the Filipino-owned internet service provider.	3.77	Agree

Table 8. On the Modernization of Cybersecurity in the Philippines

The 8th table revealed that all of the scenarios acquired a descriptive remarks of Agree.

It can be inferred that most of the respondents agreed on the needs regarding modernization of cybersecurity in the Philippines.

Question Number	Description	Weighted Mean	Descriptive Remarks
D.1	Cybersecurity in the Philippines is effective in solving cyber-related crimes and issues.	3.63	Agree
D.2	Professionals trained abroad contribute to improving the efficiency of cybersecurity in the country.	3.80	Agree

Table 9 . On the Efficiency of Cybersecurity in the Philippines

The 9th table presented that both of the two scenarios gained a descriptive remarks of Agree.

It can be deduced that most of the respondents agreed on the efficiency of cybersecurity in the Philippines.

Question Number	Description	Weighted Mean	Descriptive Remarks
E.1	Graduates of non-BS Criminology degree can pursue careers as cybersecurity expert.	3.57	Agree
E.2	There must be a leniency for the minimum standard for hiring cybersecurity and expert.	3.53	Agree

Table 10 . On the Opportunities of Cybersecurity in the Philippines

It can be glanced at the 10th table that the two (2) scenarios got a descriptive remarks of Agree.

It can be inferred that most of the respondents agreed on the opportunities of cybersecurity in the Philippines.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The researcher therefore conclude that most of the respondents were male in terms of sex, included in the age bracket of 21-25 years old, single when it comes to civil status, attained baccalaureate degree as to highest educational attainment and were employed for less than a year.

On the awareness on cybersecurity, a remark of disagree was obtained for the high chance of employment or being employed same with the public information on the existence of jobs related to cybersecurity, and the jobs related to cybersecurity is for graduates of BS Criminology only.. On the other hand, majority of the respondents agree that IT-related course graduates can be employed as cybersecurity experts.

On the challenges of cybersecurity in the Philippines, majority of the respondents got a descriptive remarks of Agree on the limitations of employment opportunities, the higher rate

of being employed abroad as cybersecurity expert, the strict qualifications for cybersecurity expert lead to reduced employment opportunities, the technical glitches of the internet service affects the performance of the cybersecurity expert, the limited if none programs and policies of the government towards cybersecurity experts, and limited trainings and certifications for cybersecurity experts.

On the modernization of cybersecurity in the Philippines, most of the respondents agreed that the backlog in data about cybersecurity adds challenge to address the problems or cases related to cybersecurity; there is a need for upgrade of the technology to strengthen the cybersecurity, and a the ownership of the internet service provider must be a Filipino to secure the welfare of the Filipino people.

On the efficiency of cybersecurity in the Philippines, majority of the respondents said that it is effective in solving cybercrime-related cases and those professionals who have trained abroad contribute to enhance the efficiency of cybersecurity in the Philippines.

On the opportunities of cybersecurity in the Philippines, majority of the respondents said that graduates of non-BS Criminology can become a cybersecurity experts and



there must be a leniency for the minimum standard for hiring cybersecurity experts.

Recommendations

The researcher presented the following recommendations:

1. A thorough information dissemination on the existence of cybersecurity, job opportunities, and opportunities for cybersecurity must be administered to give awareness to the people.
2. Cybersecurity will be more efficient if the modernization or upgrade in the technology and internet service provider will be done and preferably Filipino-owned ISP.; and
3. Strong private-public partnership, enhancement of data protection and more trainings and/seminars for cybersecurity experts will be administered.