An Assessment of CyberCrime Offenses Using Scenario Approach

Benedicto B. Balilo Jr.*, Charlemagne G. Laviña**

* API, CS/IT Department, Bicol University, Legazpi City, Philippines
** AVPAA/Dean-TIP Manila, Philippines

Abstract- The Cybercrime Prevention Act is the first law which specifically criminalizes computer crime. The law governs crimes committed online like illegal access and interception, data and system interference, misuse of device, cyber-squatting, cyber libel, identity theft, computer-related fraud and forgery, and cybersex. The awareness of students to cybercrime need to be studied to assess their level of awareness relative to cybercrime offenses because they are the most active users online so that measures can be recommended. This paper assessed the level of awareness of the 86 students enrolled in the BSCS and BSIT programs on cybercrime offenses using short description to allow high degree of understanding.

***Index Terms*:** *cybercrime, cybercrime offenses, e-commerce law*

I. INTRODUCTION

Technology posed great challenges and opportunities. The need to have access to technology and the internet are vital. Nobody can deny that the existence of this technology influence how we deal with our daily activities--the attention to vast information available and interaction via social media are now common. Nonetheless, more people are becoming not aware of the computer crimes and offenses that may affect individual activities and society in general.

According to cybercrime report the Philippines has been regarded as haven of crime committed online for many years while other countries have developed cyber warfare. It has been 13 years since the "Love Bug" virus bolstered the insufficiency of the government's policies on cybercrime [cybercrime report p11-12]. In 2012, the Cybercrime Prevention Act was signed into law and the first law in the country which specifically criminalizes computer crime, which prior to the passage of the law had no strong legal precedent in Philippine jurisprudence. The law governs crimes committed online like illegal access and interception, data and system interference, misuse of device, cyber-squatting, cyber libel, identity theft, computer-related fraud and forgery, and cybersex [1].

Many researches had been conducted and used different techniques to assess the use of computers. Scenario based approached was first illustrated in the field of computing by John Parker [as cited in 2] in a workshop attended by computer scientist, psychologists, sociologists, and lawyers. The workshop aim was to develop the concepts of unethical practices that prevail in the computer science and technology fields. The results could be used to develop proper codes of ethics. Several studies used scenario method [3-7, cited in 2]. According to [3] the scenario method which is borrowed from the ethics case approach comprises a short description of an ethical situation. An experimental subject will rate the ethics of the scenario using a single scale item with 2-to-7 point responses with endpoints of ethical and unethical. [8] used the scenario method to study gender differences in evaluating ethical dilemmas. [9] used a single scenario to study ethical decision-making associated with making illegal copies of copyrighted software. [3] utilized a multidimensional scale ethics measure to seven IT related scenarios developed by [10].

The Commission on Higher Education (CHED) order 46 series of 2012 mandates Higher Institution Education to produce thoughtful graduates imbued with values reflective of humanist orientation, analytical and problem solving skills, ability to think through the ethical and social implications of a given course of action. Graduates should have the ability and recognize the legal, social and ethical and professional issues involved in the utilization of computer technology and be guided by the adoption of appropriate professional, ethical and legal practices [12].

The purpose of this study is to assess student awareness on cybercrime offenses based on given scenario that examine the legal, ethical, and social concern of students over cybercrime laws and offenses.

II. ASSESSMENT OF CYBERCRIME OFFENSES

This presents the respondents profile and distribution and the result of the respondent assessment on cyber crime offenses based on given scenario.

A. Respondents Profile and Distribution

The respondents of the study were the BSIT and BSCS student of Bicol University. The data used was the actual enrollees registered given by the College Registrar for second semester S.Y. 2015-2016. A total of 86 (or 9.56% of the total population of the BSIT and BSCS program) respondents was considered as the population. The BSIT program has a total of 50 (or 10.2% of the total BSIT program) respondents and 36 (or 8.53% of the BSCS program) respondents were considered both for BSIT and BSCS respectively. The survey questionnaire was divided into five (5) parts which include the demographic profile of the student, awareness to cybercrime offenses, constraints encountered, lessons learned, and recommendations.

TABLE 1. RESPONDENTS PROFILE AND DISTRIBUTION

Program	BSCS	BSIT	TOTAL
First Year	12	13	25
Second Year	9	12	21
Third Year	8	14	22
Fourth Year	7	11	18
TOTAL	36	50	86

a) Scale Used. Responses to the survey instrument used the four (4) scale described in Table 2. For clarification and contextual description of the scale the following descriptions were used:

TABLE 2. SCALE USED ON SURVEY RESPONSES

Numerical equivalent	Adj Description	Range
4	Very High	4.51 – 5.00
3	High	3.51 – 4.50
2	Low	2.51 – 3.50
1	Very Low	1.00 – 2.50

4 (Very High or Strongly Agree) refers to "fully aware of the cyber crime offenses and law"; 3 (High or Agree) refers to "high in awareness of the cybercrime offenses and law"; 2 (Low or DisAgree) refers to "not aware of the offenses and its implication"; while 1 (Very Low or Strongly DisAgree) refers to "not fully aware of the cyber crime offenses and its implication".

B. Computer Offenses

a) Illegal Access. Illegal access refers to the access to the whole or any part of a computer system without right [11]. It is about entering the whole or any part of a computer system, irrespective of the communication method, directly maneuvering the system, or remotely through different network connections. In its simplest form, the access to a computer system implies an unauthorized interaction between the culprit and the targeted devices or computer components, usually by switching the computer on, using the keyboard or the mouse, printing a document, browsing folders, opening files, running software, and processing data with the purpose of acquiring information. There will also be the case of illegal access when the culprit, using his own devices or computers, finds a way to enter (to access) remote information resources (workstations, servers etc.) in the same or a different network. In order to get access to a computer system, the attacker usually tries various tools and methods, such as: password-based attacks, free-access attacks, exploiting vulnerabilities, IP or TCP hijacking-type attacks [http://www.e-crime.ero].

Table 3 shows that the awareness of respondents on illegal access was *high* (3.91). This means information relative to cyber crime laws was included in the curriculum of the institution or had been discussed as part of the classroom discussion or activities. The high awareness of the respondents could influence others that manipulating computers without authorization is not legal.

TABLE 3. SUMMARY RESULT OF ILLEGAL ACCESS

Professor Y wrote a letter to Dean BTX for the alteration of the temporary grade of student Lyeann. McGray is the assistant college registrar who has the authority of manipulating the system.		
If Professor Y intentionally accessed the college registrar system which he has no right, Professor Y is guilty of illegal access.	4.53	VH
Professor Y is not guilty if he has right to access the system	4.23	VH
If McGray took a snack and Professor Y opens the file and changed the grade of Lyeann. Professor Y is guilty of illegal access	4.44	VH
If Professor Y intentionally opens the desktop file which he has no right manipulated the system without the presence of McGray, Professor Y is guilty of illegal access	4.59	VH
If Professor Y unintentionally accessed the college registrar system, Professor Y is guilty of illegal access	3.41	L
Lyeann is guilty of illegal access if she ask a favor to McGray to higher up her grade	3.31	L
If McGray posted the file in a shared-document. If Professor Y access the document, he is guilty of illegal access	2.92	L
Overall	3.91	H

Furthermore, because of their high awareness there is a high possibility that they will be aware of the consequences that it may bring. It is noteworthy that sometimes because of many activities it cannot be evaded to know the details of illegal access. It can be noted from the data that the provision for unintentional access, files posted as a shared document, and asking favor was perceived by the respondents to be *low* (3.41, 2.92, and 3.31 respectively). Information to cyber crime laws and offenses is important so much as ICT become part of our day-to-day activities. Moreover, they are aware that accessing computers without right is cybercrime offense which is punishable by law and that anybody who manipulates the system should have proper authority.

b) Illegal Interception. Interception by technical means without right is illegal. Interception refers to listening to, recording, monitoring or surveillance of the content of communications, including producing of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring (Sec (3(m))). Table 4 shows the level of awareness of respondents on illegal interception. It can be noted from the data that the mean rating is 3.80, interpreted to be *high.* This means that the level of awareness of respondents on illegal interception is *high* given the scenario copying of files via storage media if

username and password known to both parties and distribute the same without the consent or knowledge of the other party.

TABLE 4. SUMMARY OF ILLEGAL INTERCEPTION

Gilmores and Halmore are best friends and a well known malware/virus developers. They exchanged usernames and passwords for their laptop. Anaclete is the girlfriend of Gilmores who works in an IT Solutions company.		
Assuming, they did not exchanged usernames and passwords, and Gilmores intentionally opens the files of Halmore which he has no right. Do you agree Gilmores is guilty of illegal interception	4.37	VH
If Gilmores with intent copied one (1) of the malwares they developed and gave it to Anaclete, Gilmores is guilty of illegal interception	3.87	H
If Halmore opens Gilmores laptop and copies the files and distribute the same. Do you think Halmore is guilty of illegal interception	3.65	H
Assuming, Halmore exposed the files (with malwares/viruses) in shared-documents, Gilmores intentionally opens the files and distribute the same. Do you agree Gilmores is guilty of illegal interception	3.71	H
Do you agree Anaclete is also guilty of illegal interception	3.41	L
Overall	3.80	H

It also shows from the data that any third party involved has no liability over the given scenario which is considered *low* (3.41). This means respondents are aware that illegal interception punishes only those who are principal who illegally made interception to the device.

c) Data Interference. The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses (Sec(4(a)(3)). Table 5 shows that the awareness of data interference was *high* (3.84). This means any input, alteration or deletion to the data that is necessary in the functioning of the system is considered illegal and therefore a crime punishable by sanction appropriate to the gravity of the offense.

TABLE 5. SUMMARY OF DATA INTERFERENCE

Suppose CleveRent is the programmer and at the same time the IMO Director who keeps the records of all SSS members. CleveRent mother loaned amounting to five (5) thousand pesos.		
If CleveRent alters the records of her mother making it appear that her mother has already paid the remaining balance, CleveRent is guilty of data interference	4.61	VH
If CleveRent alters the computer program so that in a specified date her mother shall be freed from all debts, CleveRent is guilty of data interference	4.48	H
If a person transmits a computer virus to the system that will affect the data, the person shall be guilty of data interference	4.32	H
If CleveRent changes the SSS contribution table with an order from her superior, CleveRent will be guilty of data interference	3.08	L
If CleveRent changes the monthly amortization (amount paid) only of her mother, CleveRent is not guilty of data interference	2.69	L
Overall	3.84	H

The access to the system without authority, alteration to the computer program on specified date and transmitting computer virus has *high* rating. This means that they are aware of the consequences if these activities will be intentionally taken into account.

d) System Interference. The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses (Sec. (4(a)(4))).

TABLE 6. SUMMARY OF SYSTEM INTERFERENCE

GSIX System is a system for the GSIS premium contributions of employees. Gutdula is a junior programmer who knows very well the system operation. The program is reading from the GSIS contribution table stored in flat file.		
If Gutdula will alter the GSIS table, he will be guilty of system interference	4.01	H
If a person transmits a computer virus to the system that will affect both data and computer program, the person shall be guilty of system interference	4.46	H
Overall	4.23	H

Table 6 shows that the awareness of respondents over system interference was *high* (4.23). This means that any system interference that affects the functioning of the computer system is punishable by law. Also, affecting both data and computer programs in the functioning of the computer system is guilty of system interference.

e) Misuse of Device. The misuse of device refers to the use, production, sale, importation, distribution, or otherwise making available, without right of: (a) device, including a computer

program, designed or adapted primarily for the purpose of committing any of the offenses under this Act, (b) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act., and the possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this Section.

Table 7 shows that the awareness over the misuse of devices was *high* (4.04). This means that respondents are aware that mere possession of any device with intent or purpose to commit an offense is illegal. Furthermore, the use, sale, procurement, importation and distribution of devices without right are also punishable under the law.

TABLE 7. SUMMARY OF MISUSE OF DEVICE

Pedro has in possession of a device/program capable of decrypting and recovering password. Juan is a friend of Jose.		
The mere possession of the program does not constitute misuse of device offense	3.89	H
If Juan use, produce, sale, procure, import and distribute or making it available without right committing a crime is guilty of misuse of device	4.09	H
It Pedro who has in possession of a device capable of decrypting password with intent to use and sell it, is an offense	3.84	H
If Juan use said device of intercepting government transaction, and reproduce the same is guilty of this offense	4.36	H
Overall	4.04	H

f) Cyber Squatting. The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration, identical or in any way similar with the name of a person other than the registrant, in case of a personal name, and acquired without right or with intellectual property interests in it.

TABLE 8. RESULT OF CYBER SQUATTING

Peterson is the owner of the company and acquired in good faith the domain name www.bloombergs.com.		
If Peterson acquires a domain name over the internet in bad faith to profit, mislead, destroy reputation and deprive others from registering the same is guilty of cyber squatting	4.22	H
If Peterson unintentionally registered a domain name and used it for philanthropic works and already registered as juridical person is guilty of cyber squatting	3.56	H
If Peterson designed the website that destroy the reputation of a person or juridical person is guilty cyber squatting	4.25	H
Overall	4.01	H

Table 8 shows that respondents awareness to cyber squatting was *high* (4.01). This means that cyber squatting prohibits any person to acquire and register domain name in bad faith whose name to be natural or juridical. Any person who took the advantage of domain registration shall follow an evaluation process before a legitimate domain name or hosting provider.

g) Cyber libel. An act committed by means of writing, printing, exhibition or any similar means with the use of a computer system or any other similar means which may be devised in the future. Table 9 shows the result of respondents perception of cyber libel was *high* (3.79).

TABLE 9. SUMMARY RESULTS FOR CYBER LIBEL

Antiley a private citizen who owns multi-billion companies. She travel's the globe two (2) times a year and do charitable activities. At summer, she distributed goods to TAYABAS foundation together with her friends.		
If Clarissa posted in her FB page "Yan c Antiley drug smuggler", Clarissa is guilty of cyber libel if all the elements are present, there must be an imputation of the crime, it must be malicious, must be in public, directed to natural or juridical person, and tend to cause the dishonor, discredit or contempt the person	4.22	H
If Brentice commented on "TOTOO YAN, KILALA KO YAN", Brentice is guilty of cyber libel	4.01	H
If Alice commented "Nagkapera yan dahil nilason niyan ang asawang KANO", Alice is guilty of cyber libel	4.18	H
If Koronel posted the statement "Hoy! President YON, 41M pagpapagawa lang ng 1 storey building, anu yan kasama na kickback", Koronel is guilty of cyber libel	3.83	H
If James posted "Alam niyo ba is Edang classmate natin nong high school kabit pala ng isang Milyonaryo". James is guilty of cyber libel	3.90	H
If Brentice like and share the posting of Clarissa, Brentice is guilty of cyber libel	3.45	L
if Alice posted on FB a picture of a traffic enforcer accepting bribe, Alice is guilty of	2.92	L

cyber libel		
Overall	3.79	H

h) Computer-related Fraud. The unauthorized input, alteration or deletion of computer data or program or interference in the functioning of a computer system causing damage thereby with fraudulent intent.

Table 10 shows the results obtained from respondents relative to computer related fraud. Respondents are highly aware that computer related fraud are activities that involves unauthorized input, alteration, or deletion to a computer data or makes an interferences that affects the functioning of the computer system and the purpose is to damage the system with fraudulent intent.

Authentication to manipulate the computer data who either participated in whole or in part without proper authorization posed *high* awareness (4.22 and 3.55 respectively) is not in any way liable of computer related fraud. Furthermore, any person who has an intent to cause damage to the system or interfere with the functioning of the system is illegal.

TABLE 10. RESULT OF COMPUTER-RELATED FRAUD

Yanky is a senior computer programmer and the Manager of Betthoven Solutions who supervises online loan application and company employees are not qualified for loan. Trish is an employee of Betthoven who needed money for her mothers' operation. Trish made an alteration to her mother contribution and applied for loan renewal.		
If Trish made an input, alteration and deletion to the system causing for the system to shutdown, Trish is guilty of computer-related fraud	4.20	H
Trish is guilty of computer-related fraud because there is an input, deletion, and alteration of the data or interference to the functioning of the system and the purpose is to damage the system with fraudulent intent	4.22	H
If Yanky made an authorized changes to the annual loan rate that affect the entire computation of the system, Yanky is not guilty of computer-related fraud	3.55	H
Trish is not guilty of computer-related fraud	2.84	L
Overall	3.70	H

i) Computer-related Forgery. The input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible, or the act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

TABLE 10. SUMMARY RESULT FOR COMPUTER-RELATED FORGERY

BYS is an online Barangay Youth System. Gloria is a Barangay Secretary who is authorized to use the system. Yano is a Barangay Kagawad in-charge of Committee on Sports and Development. In order for the youth to qualify for the Municipal Basketball Competition Gloria made an alteration changing the age to be legal (18 years old). Said certification was known to Barangay Kagawad and still signed the certification.		
Gloria is guilty of computer-related forgery	3.66	H
If Gloria made no modifications, Gloria is not guilty of computer-related forgery	3.83	H
The input, alteration, or deletion of any computer data without right resulting to an inauthentic data are elements of computer-related forgery	4.00	H
An officer who has a knowledge of an inauthentic data and confirms it's an authentic one is an example of PASSIVE computer-related forgery	3.84	H
An officer who made an input, alteration or deletion to data resulting to an inauthentic result is an example of ACTIVE computer-related forgery	3.97	H
Barangay Kagawad is guilty of computer-related forgery	3.22	L
If Barangay Kagawad has no knowledge of the changes made by Gloria, Barangay Kagawad is still guilty of computer-related forgery	2.84	L
Overall	3.62	H

j) Cybersex. The willful engagement, operation, control and maintenance, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity with the aid of a computer system, for favor or consideration.

In table 11, the awareness of respondent was *high* (3.98). This means they are aware that cyber sex is illegal, an offense punishable by law and that the elements therein are fully satisfied.

TABLE 11. SUMMARY RESULTS FOR CYBERSEX

Assuming Mr. Cleanse offered Sally Php 40,000 to have cybersex, but Sally refused. Due to unavoidable circumstances Sally needed money no choice but to accept Mr. Cleanse offer.		
Both Sally and Mr. Cleanse are guilty of cybersex	4.28	H
Sally is guilty of cybersex	4.05	H
Mr. Cleanse is guilty of cybersex	4.35	H
If Daniel offered Sally to others to gain 5% commissioned, Daniel is guilty of cybersex	4.23	H

Both are guilty if the elements of cyber sex must be present thus, there must be a willful engagement, maintenance, and control of the lascivious and exhibition of the sexual organs, lascivious activity is done with the aid or through the use of computer system, and the activity is done for a favor or consideration.	4.23	H
Any of said elements not present is not guilty of cybersex	3.51	H
Cybersex punishes those who are engage in business or operation of any lascivious and exhibition of sexual organs	4.12	H
If Sally is a prostitute, Sally is guilty of cybersex	3.69	H
B a married man and D single consented to videotaped their doings and uploaded via Youtube, B and D are guilty of cybersex	3.95	H
If Sally and Mr. Cleanse are married couple doing cybersex, both are guilty of cybersex	3.41	L
Overall	3.98	H

Respondents are not fully aware that there is legal cyber sex and there had been law that sets limitations and decriminalized such act like prostitute.

C. Constraints Encountered.

Respondents were asked what constraints they have encountered about their awareness to cybercrime law. Table 12 shows that respondents were provided limited information (2.28) about cybercrime offenses as the highest constraint, followed by it was never discussed in the classroom (2.36), not reading computer related laws (2.52), they have no time reading computer related laws (2.96), and studying said law is not needed in their field (3.65).

TABLE 12. CONSTRAINTS ENCOUNTERED OVER CYBER CRIME OFFENSES AND LAWS

limited discussion in the classroom	1
not discussed in the classroom	2
not reading computer related laws	3
no time to read computer related laws	4
not needed in my field	5

D. Lessons Learned

Table 13 shows the results what lessons did the respondents learned after answering the survey questionnaire. It revealed that after answering the questionnaire respondents are enlightened what are cyber crime offenses that are punishable under cyber crime law (1.92). Others said it widens their awareness (2.15), makes them aware of the effect that may be caused by cyber crime law (2.56), helpful enough for students like them (3.15).

TABLE 13. LESSON LEARNED AFTER ANSWERING THE SURVEY QUESTIONNAIRE

enlightens me about some crimes and offenses under cyber crime law	1.92	1
widen my awareness on cyber crime law	2.15	2
makes me aware of the effect that may be caused by cyber crime law	2.56	3
helpful enough for a student like me	3.15	4
not so much helpful, just a little bit	3.77	5

E. Recommendation. Respondents were asked of the possible recommendations on how this study will help them to be aware not only cyber crime laws but topics which are relevant to their field of specialization. In Figure 13, the most recommended mechanism that respondents would like to emphasize is providing lectures and seminars on computer related crime and laws (1.98). The second recommendation is to have a discussion focus inside the classroom (2.16), include in the University calendar of events (2.97), use social media and create a forum or group that is focused on the awareness of cyber crime offenses and laws (3.19), and improve the course syllabus (3.24).

TABLE 14. RECOMMENDATION TO INCREASE AWARENESS TO CYBER CRIME OFFENSES AND LAWS

provide lecture and seminar on computer related crime and laws	1.98	1
Discuss in the classroom	2.16	2
acknowledge/include in the event of CS/IT week or other University Wide activity	2.97	3
create a forum, group on social media with aim to help students aware of cyber crime laws	3.19	4
improve course syllabus	3.24	5

III. CONCLUSION

Using cybercrime offense-scenario approach the researcher allows to evaluate responses closed to the understanding of the respondents. The easiness and description of the scenario gives respondents to visualized cybercrime offenses.

E-commerce law is among the laws that govern cyber crime offenses. The law governs crimes committed online like illegal access and interception, data and system interference, misuse of device, cyber-squatting, cyber libel, identity theft, computer-related fraud and forgery, and cybersex. Furthermore, respondents posed higher awareness through situations and example.

IV. RECOMMENDATION

The awareness to existing laws is a must that everybody should be aware of. To widen its dissemination, an inclusion of cyber crime related activities is much beneficial if properly presented and disseminated to schools and to the community in general.

V. ACKNOWLEDGEMENTS

Thank you to Dr. Charlemagne Laviña for the great motivation and encouragement for without him this paper will not be realized, Dr. Bartolome Tanguilig for the support given to be part of the TIP-DIT program and to Technological Institute of the Philippines community.

VI. REFERENCES

[1] Republic Act 10175. Official Gazette. "AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES". Approved by President of the Philippines BENIGNO S. AQUINO III on September 12, 2012

[2] M. Masrom, Z. Ismail, et. al. *An Ethical Assessment of Computer Ethics Using Scenario Approach*. International Journal of Electronic Commerce Studies Vol.1, No.1 , pp.25-36, 2010

[3] T. S. Ellis and D. Griffifth, The evaluation of IT ethical decision making in marketing. *The DATA BASE for Advances in Information Systems*, Winter, 32(1), 75-85, 2001.

[4] A. G. Namlu and H. F. Odabasi, Unethical computer using behavior scale: a study of reliability and validity on Turkish university students. *Computers & Education*, 48(2), 205-215, 2007.

[5] C. M. Hanchey and J. Kingsbury, A survey of students' ethical attitudes using computer-related scenarios. *Proceedings of the Conference on Ethics in the Computer Age*, November, 2-6, 1994.

[6] R. Guthrie, Ethical scenarios, http://newton.uor.edu/FacultyFolder/RGuthrie/courses/escenarios.html, 1998.

[7] S. Athey, A comparison of experts' and high tech students' ethical beliefs in computer-related situations. *Journal of Business Ethics*, 12, 359-370, 1993.

[8] J. Kreie and T. P. Cronan, How men and women view ethics. *Communications of the ACM*, 41 (9), 70-76, 1998.

[9] J. Y. L. Thong and Yap, C. S. Yap, Testing an ethical decision-making theory: the case of soft lifting. *Journal of Management Information*, 15(1), 213-237, 1998.

[10] B. W. Lifick, Analyzing ethical scenarios. *Proceedings of ETHICOMP95 Conference*, March 28-30, De Montfort University, Leicester, UK, 1995.

[11] Republic Act 10173 "Cybercrime Prevention Act of 2012". Chapter II Section 4(1)

[12] LAVINA, C.G., "Social, Ethical, Legal, and Professional Issues in Computing" with complete explanation of the PHILIPPINE CYBERCRIME LAWS. ISBN:978-621-406-018-4 copyright 2015.

AUTHORS

Benedicto B. Balilo Jr. He is currently taking his Doctor in IT as CHED scholar at Technological Insitute of the Philippines (TIP). He is a graduate of Master in Information Technology (MIT) program from the University of the Cordilleras in 2015 as a CHED Scholar and earned his Masters degree program in Business Administration (MBA) at Aquinas University of Legazpi in 2012 and Bachelor of Science in Computer Science at DCC in 1994. He also earned units in Master in Information Systems (MIS) at UPOU-LB and Bachelor of Laws (LLb) at Aquinas University of Legazpi.

At present, he is currently employed as Assistant Professor I and a former College Extension Coordinator of the College of Science, Bicol University, Legazpi City. He is the current Philippine Society of IT Educators (PSITE) Region V President and a former Municipal Councilor (9 years) and Consultant of Sto. Domingo, Albay. A member of various professional organizations such as PSITE, PeLS, NMYL, and PCL. Email Address: jrbalilo@yahoo.com / 0998-5463-563

DR. CHARLEMAGNE G. LAVIÑA is presently the Asst. Vice President for Academic Affairs (AVPAA) and concurrent Dean of the College of Information Technology Education and Graduate Programs of the Technological Institute of the Philippines (TIP-Manila). He earned his PdD in Information Technology Management from Letran Calamba in 2006; Master of Science in CS (MSCS) from AMACC-Makati in 2001 and BSCS from the Laguna College of Business and Arts-Calamba in 1994. He is a member of CHED Regional Quality Assurance Team (RQAT)-NCR and was designated as one of the National Pool of Technical Assessors for IT Education. He is also a PACUCOA Accreditor, Assessor for Institutional Sustainability Assessment (ISA) and a program evaluator of the PCS Information and Computing Accreditation Board (PICAB).