ISSN No:-2456-2165

Cybersecurity and Cryptocurrency Awareness in Finance

Engr. Raymond C. Medina, PECE, ACPE Engr., APEC Engr., ASEAN Engr.
SSCR MBA Student2nd Semester 2021-2022

San Sebastian College-Recoletos
2114-A Claro M. Recto Avenue, Zone 040 Barangay 390, Quiapo,
Manila Tel. Nos.: 734-8931 to 39, loc. 158

INSTITUTE OF GRADUATE STUDIES
Executive Education for Social Innovation
LEARN. LEAD. INNOVATE. SERVE.

Abstract:- Why care about Cybersecurity? Referencing the book of National Academics of Sciences, Engineering and Medicine about "AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY: SOME BASIC CONCEPTS AND ISSUES published on 2014; Cybersecurity has been an issue of public policy significance for a number of decades. For example, in 1991 the National Research Council wrote in Computers at Risk:

We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. (p. 7)

The continuous evolution of information technology gives rise to the digital format of the fiat currencies that we have, of which some amounts we carry and place them in our wallets or withdraw thru banks either via a teller or automated teller machine. These digital currencies are used in on-line internet transactions, and, other e-commerce activities. Furthermore, e-commerce lead to boundaryless world where business transactions and payments can be made anytime and anywhere. However, the value of respective currencies poses a challenge in the transactions. Thus, the rise of Cryptocurrency has emerged. The need for a "flattening the world" approach in the boundary less electronic commerce has made many to consider the use of cryptocurrencies in their business transactions worldwide. However, is it safe and stable?

I. INTRODUCTION

The world has totally evolved driven by the speed of changes in technology and the daily innovations that is being introduced. The entire dynamics of the industry was not left untouched, thus leading to INDUSTRY 4.0. Information data has become the new "gold" right now. Data has become the fourth utility after air, water, energy. Money has already been converted to have digital equivalent that can be used for commerce whether it is in a form of information and some even the consider virtual currencies.

The advantage of these evolution in the finance industry has been emphasized the past two years where the world has been in the state of pndemic because of Covid 19. During these period, specially during the peek of infection, business and commerce has to continue to resist the effects of recession. On line transactions and commerce has saved thru a major contribution in these very trying times. While the world enjoys these innovation, a new threat has further emerged,stealing of financial informations thru our internet accounts. The focus of Cybersecurity has been a hot topic universally most specially at this time of pandemic. Cybersecurity covers all sectors of the country and poses a great importance and dynamics that may affect economy such as energy, transportation, telecommunication, banking, finance, business, health and governance. It NOT just ticking a box nor using an anti-virus software.

When the basic services of the society are stopped such finances, telecommunications, water , fuel, power, travel, and supplies because of facility technical issues due to a cyber-attackwhich causes inconvenience or economic distress.

Destruction of or damage to physical property: *Individual cyber physical systems* – are personal technology items whether used by an organization or company or individual person.*Critical infrastructures* – are the countries or society's basic infrastructures such as the energy, telecommunication, transportation, banking and finance.*Public confidence*–lost of trust to governance when

ISSN No:-2456-2165

cybercrimes are increasing.*Threats to national security and cyber war*–national defense, intelligence, weaponry and economy relies heavily on information technology and communications systems such as command and control, logistics management, and, administrations. Thus, any attempt of cybercrime will be treated as grave threats and may results to domestic and international wars.

Thedomestic cyber incidents in the average of ten days has an average of two (2) per day of which 75% of the attacks were on private, and 25% percent are on government institutions and/or agencies.

This year, the Data Breach Incident Report (DBIR) 202 has reported that it has analyzed 79,635 breaches. Of which 29, 207 of passed their quality standards of a qualified cyber incident, where 5,258 are confirmed data breaches. Sampled from 88 countries in the world where 11 are in the main industries. See information below:

DBIR is under the copyright and ownership of Verizon, a telecommunication company in the United States. It is assumed that data published in the said report are based ONLY on their own telecommunications infrastructure, and/or related companies with legal arrangements, and/or ownerships

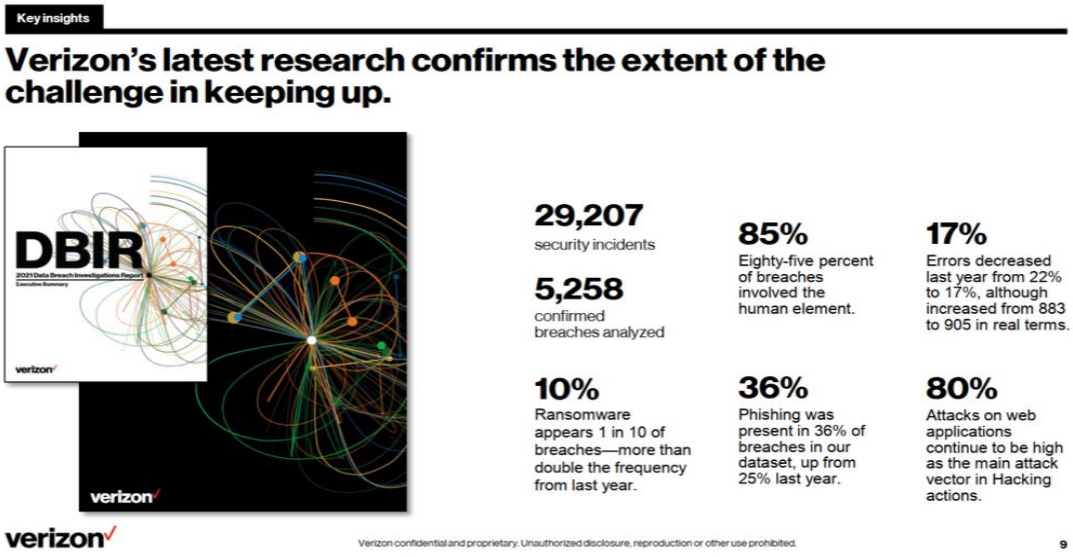

Fig. 1: 2021 DBIR Report

On the recently conducted Southeast Asia Internet Governance forum, as I personally attended in representing the Department of Information's and Communications Technology Cyber security Bureau, the following information were discussed and provided:

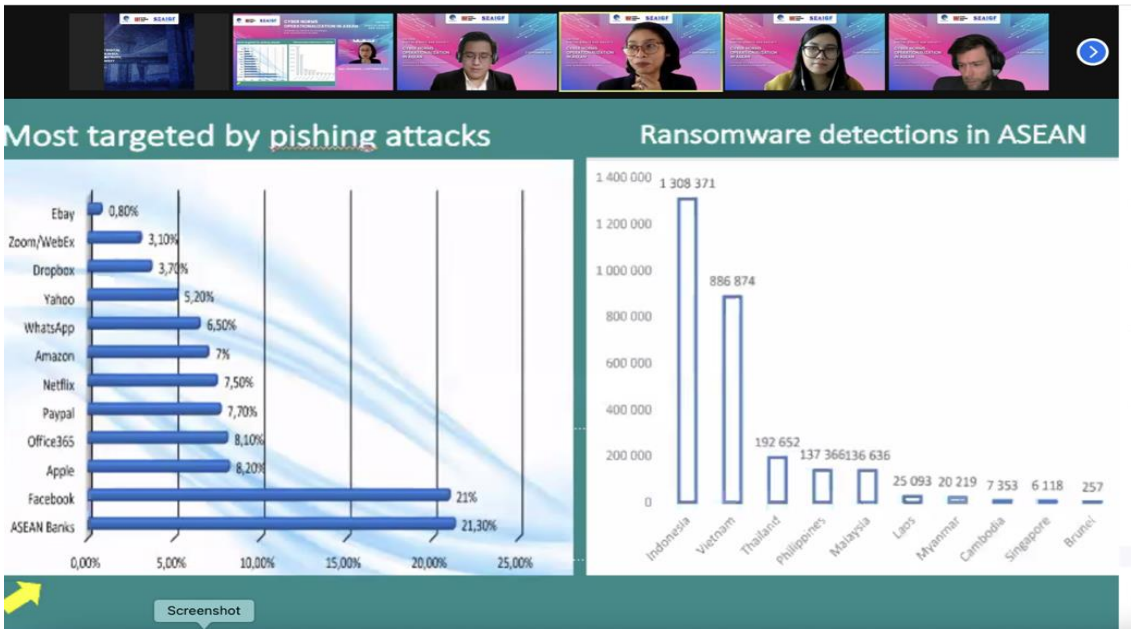

Fig. 2: SEA Internet Governance Cyber Attacks Report

ISSN No:-2456-2165

Clearly, ASEAN banks, which includes the Philippines, are the most targeted by phishing attacks. The Philippines is the fourth most number of detected ransomware detected in the ASEAN countries. *South East Asian Governance Forum held at Bali, Indonesia on September 18, 2021.*

Further, the emergence electronic commerce gave rise to the full potential use of the digital currencies and cryptocurrencies. Financial technology is an industry that uses technology and digital methods for financial services and activities. Often these methods bypass traditional financial institutions such as banks and physical money in favor of cashless transactions and digitally integrated software.

Fintech is heavily reliant on high levels of internet penetration, in particular mobile internet usage, to deliver services to a wide range of users. New applications, products or processes that focus on delivering financial services via the internet can be considered part of the fintech industry.Smartphones, mobile banking, investment apps, and cryptocurrencies are all examples of fintech aimed at making it easier for the average person to access financial services.

As a mostly young, tech savvy populace with a fast-growing economy. With over 30 million smartphone users and new government investment, the country has seen an explosion of new technology developments and innovations. The Philippines is in a good position to take advantage of the fintech with reference to the latter statement.

Bangko Sentral ng Pilipinas (BSP), the country's banking regulator has ordered financial institutions to reinforce their information technology systems to better protect their institutions and clients from cyberattacks, which is growing alongside the increase in digital transactions during the ongoing pandemic.

The banking industry is aware of the need to manage the balance between stifling innovation and ensuring accountability in respect of and compliance with notable public policies on data privacy, investor protection and redress, anti-money laundering and cybersecurity — areas where the fintech market is perceived to be more open to abuse. Rationalizing existing regulations and refining new and upcoming ones remain key challenges faced by local regulators tasked with fostering a progressive and collaborative environment within which the fintech market in the Philippines

In order to provide financial services, fintech companies collect the data of their customers such as name, date of birth, address, gender, nationality, PINs, passwords, social security details, bank account details, and more. Recently, they've also begun drawing information from non-traditional sources such as alternative data. These include web browser history, behavior on social media platforms (their posts, interactions, and response to certain issues), and psychological profiles.

Alternative data is rising in popularity because it provides information about an individual that cannot be captured by traditional methods. It helps banks, lenders, and financial institutions determine the creditworthiness of an individual. For instance, if a certain user uses their virtual wallet to pay monthly bills before the due date, it's a clear indication of their ability to repay loans on time.

However, extensive, and aggressive data collection introduces numerous security and privacy issues. For one, it raises questions as to whether people are aware that companies are harvesting their online behavioral data. Fintech companies also become attractive targets for cybercriminals due to their collection of valuable personal information.

Despite the rising importance of Fintech, relevant regulatory structures also exist to manage risks and at times, create a patchwork of legal barriers that impose various obligations on firms. These sectorial laws and regulations are applicable across areas such as privacy, cybersecurity, and information security.

COVID-19 has increased demand for e-Commerce in the Philippines. While the younger population was already open to online shopping, the need for social distancing has pushed the cash centric and face to face shopping culture towards a more digital one, and this is expected to continue. What is lacking is proper digital and logistics infrastructure to truly enable a digital economy. There needs to be higher bandwidth capacity to service the retail market.

As growth in cross-border B2C trade expands, hindrances to regional trade are brought to light. Common concerns include internet access, cybersecurity, customs rules and taxation, currency exchange, and the returns process. All these points towards the need for regional investment in connectivity, not just in terms of technology and infrastructure, but also in the necessity of forming regionally recognized cross-border standards and regulations. Thus, consideration of cryptocurrency.

Apart from technology, social adoption hinged on education and security, facilitative legal and institutional environment, and efficiency of payment and delivery systems contribute to the expansion of e-business.

II. STATEMENT OF THE PROBLEM

Like any organic or biological viruses, computer viruses and infections spreads via an individual to small group of a population, until reaches an entire organization if not properly managed and mitigated. Further, there are even computer infections that only presents itself when the attack by hackers or cybercriminals is already executed. The longest recorded data before the breach was detected was 250 days as reported by *Cost of Breach Report 2021 thru a webinar by Brightalk presented by Crowdstrike*.

Further, Figure 1 above of the Data Breach Incident Report for 2021 mentions based on their analyzed data of breaches, 85% of the incident involves human element. This means that whether the breach incident is intended or merely

ISSN No:-2456-2165

unintentional because of lack awareness or cybersecurity understanding. Everyone is obviously exposed to all of the threat because of the presence in internet, personal uses like banking and other electronic commerce.

The dangers posed by fintech to consumers can be broadly categorized around loss of privacy; compromised data security; rising risks of fraud and scams; unfair and discriminatory uses of data and data analytics; uses of data that are non-transparent to both consumers and regulators; harmful manipulation of consumer behavior; and risks that tech firms entering the financial or financial regulatory space will lack adequate knowledge, operational effectiveness, and stability. (https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_151_final.pdf)

While the works has been aggressive in utilizing financial technologies, currency has been the major challenge of transaction. As a solution, cryptocurrencies has been introducedas one of the forms of fintech and getting more popular.Cryptocurrency technical aspects such as encryption mechanisms involves a complex algorithm focused on security known as blockchain. However, since it is done by an unknown individual, CAN WE TRUST IT? What is the guarantee that the code is secure without seeing the source code perse. How can we be assured of cybersecurity in the utilization of such fintech? How vast is the acceptance of such currency that it can be used for exchanges? And finally, the treatment of store value during exchanges, will be fair and properly cost?

Legality, Stability, Transparency of cyrptocurrency are the constant issue brought out in uskng cryptocurrencies. Note that it is decentralized and unregulated by the government. With rise of its popularity and slow accpetance, it has been the currency for illegal transactions, and target of cyber attacks. Without propoper governance, it is also a common tool being used for scams.

Without fiscal policies, the use of cryptocurencies will harm the system and rmpant tax evasions may happen. Large amount of transactions may happen without government shares will have an economic impact to a state.Balance sheets of corporations and businesses will have mismatches specially on the currencies, thus annual tax reports are easily altered and manipulated. Chain reactions could lead or pose a major risks to global financial stability.

On the investors side of cryptocurrencies, they should be very watchful of its stability. Again, this currency is unregulated and dependend only on ¨trust between a community of users and investors¨. Once such ¨trust¨ is lost and global sovereign interventions have been in effect, such may result to catastrophic downfall of value. Finaly, what is the true source of its value?

III. RECOMMENDATION AND DISCUSSION

The history of fintech and digital money has started way back in the 1950's where the first credit cards were used. Communications technology has evolved and interconnectivity has been introduced thus automated banking was introduced. In 1998, PayPal was introduced as the first digital wallet in the internet.

*Fintech, or financial technology, is the term used to describe any technology that delivers financial services through software, such as online banking, mobile payment apps or even cryptocurrency.*https://www.uschamber.com/co/run/business-financing/what-is-fintech

Types of fintech's are mobile wallets and payments apps, crowdfunding platforms used for investing whether to businesses, individual or products, cryptocurrency being the most scrutinized digital equivalent of money, Robo-advisors for portfolio management, stock trading apps, and insuretech as digital registration of insurances.

The difference between Digital currency is that it the digital format of our fiat money whose purchasing power and value is supported and regulated by a sovereign thru its central bank. While, the purchasing power of a Cryptocurrency is virtual, derived from a community of users.Cryptocurrencies are unregulatedand un-supervised by any sovereign state. Currencies are durable, easily tradeable, has discrete units, and a store value. Currencies are based on gold, fiat or the physical currency we have been using, the digital currencies approved and regulated by the central bank using the same value and termed as the fiat currency. Digital currencies can also be cryptocurrencies.

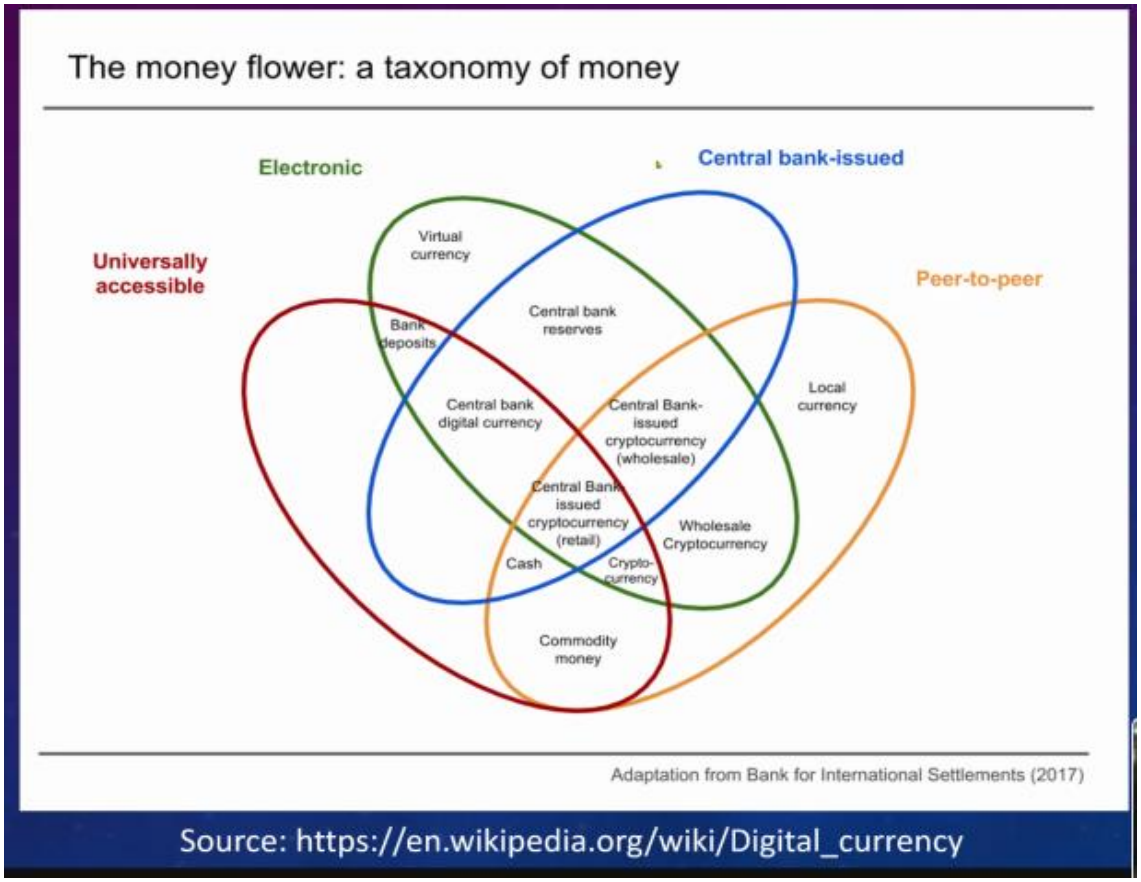

Fig. 3: The Money Flower

When we talk about digital currencies, the technical aspect will always be a point of consideration, in this case a special algorithm of coding is being used for security purpose known as Blockchain Technology. Blockchain by definition is a system of recording information in a way that it is ddifficult or impossible to change, hack or cheat the system.https://www.google.com.ph/search?q=blockchain+technology&ie=UTF-8&oe=UTF-8&hl=en-ph&client=safari

Blockchain technologies are used in the digital banking industry and are commissioned by private regulated banks on technology contractors. Considering that these privately owned and regulated banks would give us more confidence and trust in utilizing the system and technology. However, said trust will be different if you are to invest and use cryptocurrencies. Without regulation, there is no government oversight on the safety and execution of these cryptocurrencies. The control of the stability is dependent on private process and execution and just a matter of trust and confidence in the "product". How the source code of the blockchain is created, who is the contractor, and even the whole personalities behind the cryptocurrency remains as shadows. Thus, cryptocurrencies are preferred payments for illegal transactions and businesses. Cryptocurrencies are the monetary values being used in the " DARK WEB" where e-commerce for criminals resides. Dark web are the larger part of the ocean when we speak of the internet and world wide web horizon and are not commonly being accessed. A different type of browser is used in accessing the sites on this horizon where high caution for safety and experience is a must when you intend to access.

In digital banking or financial technology once you have understood the dynamics, process and regulations it will all boil down to a common ground of topic importance, and that is trust and safety. Therefore, in order to achieve trust and safety we need to be assured of security of our money and investments. Emphasizing the definition of Cybersecurity as per Republic Act (RA) 10175 otherwise known as THE CYBERCRIME ACT OF 2012, *as the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*, requires of a whole organization and whole government approach. While technology evolves every day, the threatsurfacein the cyberspace as well widens. It is very important that one has the complete understanding of the capabilities of the technology, and the danger of constant exposure to the threats everytime one connects to the internet.

One must have complete understanding on what and where is the money coming and going to. It is always highly suggested to invest in regulated, governed and supervised investments, including currencies. While there are advantages of cryptocurrencies, the trust and confidence level should not be totally equated to the benefits of other fintechwhich are under sovereign regulations. Consider long term stability forecast and global acceptance of the cryptocurrency because it will dictate the stability of its value.

Finally, once everything is technically and financially understood about fintech, it is highly recommended to provide in depth seminars/webinars about cybersecurity. Suggested topics involve what are the Cybersecurity Landscape and attack surfaces in the Philippines, The Philippine Government interventions in cybersecurity, Digital Parenting, Forecast of Cybersecurity Threats to name a few.Data Privacyis also highly recommended because people needs to understand when it ok to send out or share personal information of oneself and others to on line transactions. One must do a VERY DEEP research on investing, do not rely on simple e-mail invitations, nor mere invites from close friends to invest or store money in fintech's. Stand in the shoulder of giants is a good metaphor to consider in fintech and e-commerce.

Further, people needs to understand that connecting to the internet is NOT a complete freedom. There are rules and regulations that needs to be followed and understand by everyone. Check regulation announcements from the Department of Informations and Communications Technology, the Department of Finance, and Banko Sentral ng Pilipinas to update your knowledge on Cybersecurity and security of investments.

The interconnected or boundary less world will continue. The pandemic of Covid 19 evolved us to the "NEW NORMAL" of the society where the dynamics of school, work, commerce, and many more has changed. Physical presence is no longer necessary to gain knowledge or graduate, work and produce an output, submit or gain information, or earn money. Do we need a basis? Just look around us, is the more than 2 years of the pandemic not enough…?

As the cyberthreat surface grows while technology is continuously improving and evolving it is imperative that all individuals are updated. Always informed of the new threats and mitigation procedures thru various attendance to cybersecurity awareness programs particularly on government provided ones such as Department of Information and Communications Technology, Cybersecurity Bureau. Information sharing and organizational preparedness because RESILIENCY and RECOVERY is the KEY, based on the National Institute of Standards and Technology (NIST) cybersecurity framework. An organization should be able to establish management, procedures, risk assessment, continuity plans, and updated technical capabilities, and including cybersecurity in their priorities.

Cyber threats will always be there. Cyber-attackscan never be stopped, it is not a matter of what, but a matter of WHEN.

IV. CONCLUSION

The matter about Cryptocurrency and Cybersecurity all boils down to the matter of empahasizing TRUST.

Fact is, any currency in the world is based on the matter of legitimacy and acceptance of everyone in the world. Government recognition and regulations of currencies in different countries in the world setups the matter of confidence of people investing and using these currencies. Thus, TRUST is the root cause of stability of these currencies by the different country's.Trust in the value based on the economic capacity of the country. Trust on the value stability based on the mutual trust and acceptance of other countries as well. This matter of principleis the basis of the cryptocurrency investors and users, their main selling point to TRUST the use of their digital currency. However, a matter of group of individuals, nor groups, nor investors will immediately bring out TRUST to all. People will always seek confidence when there is government legislation and regulation, as what the fiat currency have. Further, there is a matter of security.

Fiat money whether in the application of financial technology are still secured because of government regulation. While cryptocurrency must require a lot of understanding, learning and awareness in cybersecurity. The world is still getting used to the industrial evolution 4.0 where most are already technology driven and dependent in the internet. A "honeymoon" stage where almost everything are good, but blindsided by the fact that there are individuals taking advantage and criminally acting digitally.

The matter of cyber security must be guaranteed and prioritized by all legislators and regulatorsin all the countries before trust and confidence in the cryptocurrency will be gained.

REFERENCES

[1.] Philippine Law, (2012). Republic Act 10175 :The Cybercrime Act of 2012. Republic of the Philippines.
[2.] Philippine Law, (2012). Republic Act 10173 :The Data Provacy Act of 2012. Republic of the Philippines.
[3.] CISCO. What is Malware?, https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html
[4.] Tatu Ylonen. SSH - Secure Login Connectivity Proceedings of the 6th USENIX Security. Website. https://www.ssh.com/academy/ssh
[5.] 2021 AO Kaspersky Lab. Brute Force Attack: Definition and Examples. Website. https://www.kaspersky.com/resource-center/definitions/brute-force-attack
[6.] 2021 AO Kaspersky Lab. What is Social Engineering. Website. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering
[7.] 2021 NortonLifeLock Inc. What is a distributed denial of service attack (DDOS) and what can you do about them:. Website. https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

[8.] Verizon Inc. 2021 Data Breach Invetigations Report. Website. https://www.google.com.ph/search?q=dbir+report&ie=UTF-8&oe=UTF-8&hl=en-ph&client=safari
[9.] 2021 South East Asia Internet Governance Forum:. Bali, Indonesia.Website. https://seaigf.id/
[10.] IT Security Risk Survey 2017, global data.
[11.] Cell phones a harder hack target than computers, FireEye's President says, PUBLISHED SUN, APR 19 20159:00 AM EDTUPDATED SUN, APR 19 20159:00 AM EDTTrent Gillies; https://www.cnbc.com/2015/04/19/cell-phones-a-harder-hack-target-than-computers-fireeyes-president-says.html
[12.] Laptop vs Tablet published by Tech Advisor on October 30, 2018 by Martyn Casserly; https://www.techadvisor.com/feature/laptop/laptop-vs-tablet-3685888/
[13.] Cybersecurity in the Modern World: Public WIFI are we at risk by Caleb Townsed;https://www.uscybersecurity.net/public-wifi/.
[14.] Business insider article April 3, 2021:533 million Facebook users' phone numbers and personal data have been leaked by Aaron Holmes; https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4
[15.] Kasperksy.com Resource Center:Online Video Calls & Conferencing: How to Stay Safe from Hackers
[16.] https://www.kaspersky.com/resource-center/threats/video-conferencing-security-how-to-stay-safe.
[17.] Cybersecurity Projections for 2022 , Brightalk
[18.] Cost of Breach Report 2021 by Brightalk presented by Crowdstrike.

Sources

[19.] 1991 National Research Council
[20.] Verizon 2021 Data Breach Investigation Report
[21.] South East Asian Governance Forum https://www.seaigf.id
[22.] US Chamber of Commercehttps://www.uschamber.com/co/run/business-financing/what-is-fintech
[23.] Harvard Kennedy School, Digital Technology Risks for Finance: Dangers Embedded in FinTech and Regtech; https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_151_final.pdf
[24.] CNBC Digital Currency vs Cryptocurrency; https://www.cnbctv18.com/cryptocurrency/digital-currency-vs-cryptocurrency--whats-the-difference-12611902.htm
[25.] We have no conflict of interest to disclose.
[26.] Correspondence concerning this article should be addressed to **Engr.Raymond C. Medina**, at SSCR Manila Institute of Graduate School. Email: rc.medina@sscrmnl.edu.ph

Submitted to: DR. DENNIS SANDOVAL for MCC 103 (FINANCIAL MANAGEMENT)

RESEARCHERS BIO

Raymond C. Medina is a Professional Electronics Engineer with over twenty five(25) years of extensive experience in various engineering fields. He has his own consulting firm involved with different construction projects here in the Philippines and abroad. Raymond is an expert in design and project management of MEPF, IT, Electronic Security and Life Safety; IT infrastructure design; cabling systems; security systems; transmission line designs; and, logistics, sales and project management. *Also working with the Department of Information and Communications Technology (DICT) Cybersecurity Bureau office of the Director as a Highly Technical Consultant for project implementation, policy formulations, etc. A Cybersecurity expert licensed ASEAN Chartered Professional Engineer, ACPE Engineer, and ASEAN Engineer.*

Education:

College/University	Degree/Title Obtained	Inclusive Dates
Mapua Institute of Technology	Bachelor of Science in Electronics and Communications Engineering	1994-1998
San Sebastian College	*Masters in Busines Administration*	*2021-Present*
San Sebastian College	*Juris Doctor*	*2021-Present*