Financial and Social Costs Perspective Impacts of Cybercrime in the UAE: Policy-Guidance Addressing the Problem in Piecemeal Approach

International Journal of Economics, Business and Management Studies
Vol. 9, No. 2, 89-103, 2022
e-ISSN: 2226-4809/p-ISSN: 2304-6945

(Corresponding Author)

Akim M. Rahman[1]
Saadi Islam[2]

[1] *Department of Economics, Canadian University of Bangladesh, and Social and Economic Research Institute, Bangladesh.*
Email: akim_rahman@hotmail.com
[2] *American International University-Bangladesh, Bangladesh.*
Email: saadi.islam@gmail.com

ABSTRACT

Today's technology-driven human-society(s) country-wise are counted more than ever before where UAE-society is no exception. Tech-users here compete for comparative time-saving-options for marginalizing operating-cost. It has resulted huge data-usages, high-number of users & devices, which has attracted criminals for taking advantages, which is known as cybercrime. Addressing cybercrime, the UAE, like other countries, is not out of controlled by laws. However, laws like cybercrime for its society are not always for absolutely eliminating the crime. Thus, besides cybercrime-law in place, UAE needs *piecemeal* approach in practice where one department may vary from approaches of other-department. With awareness about risky online-behaviors & options, tech-users as defenders need to invest own-efforts. This study has laid out foundation of the proposal, *Akim's Model-2021*, using Theory of Consumer Choice & Behaviors and Welfare Analysis. Tech-user's actual utility-received is the sum of utility-received from *awareness & own-effort* and utility-received from cybercrime-law. Any changes to services-received from joint-efforts may risk tech-user to be a victim. Welfare analysis shows tech-user's actions - *awareness & own-effort*, besides cybercrime-law can create Net Social-gain, which depends on tech-user's own-actions. Tech-user's economic-surplus is greater than government-expenses for implementation of cybercrime-law in UAE. Net-loss to the UAE is the sum of deadweight-loss and net-loss to tech-producers for underutilized resources.

Keywords: *Awareness cybercrime, Own effort, Piecemeal approach, Sense of responsibility.*

DOI: 10.55284/ijebms.v9i2.718
Citation | Akim M. Rahman; Saadi Islam (2022). Financial and Social Costs Perspective Impacts of Cybercrime in the UAE: Policy-Guidance Addressing the Problem in Piecemeal Approach. International Journal of Economics, Business and Management Studies, 9(2): 89-103.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
History: Received: 4 August 2022/ Revised: 19 September 2022/ Accepted: 6 October 2022/ Published: 13 October 2022
Publisher: Online Science Publishing

Highlights of this paper:

- Today, Middle East countries are increasingly investing in ICTs, but it is no free from happening cybercrime.
- Addressing the problem, besides cybercrime laws in place, Middle East countries need piecemeal approach in practice.
- Thus, tech-user's actions - awareness & own-efforts can create Net Social-gain in tech-driven middle eastern society.

1. INTRODUCTION

Today's humankind lives in world of business-mentality with technology-driven lifestyles where services are conducted in multi-faucets, competitive and rationality manner (Rahman, 2018). In this technology-driven-world, humankind counts time-values more than ever before where the United Arab Emirates (UAE) society is no different. Thus, decision-factors convenience and cost-effectiveness have led individuals, organizations, agencies, or businesses welcoming the Information Communication Technology (ICT)-facilitations for using in multi-faucets.

As a result, meeting society needs, multi-sectors including service sector like banking has been modernized (Rahman, 2021b). Here customers compete for comparative time-saving-option(s) for marginalizing its operating costs. This progression of ICT utilizations in other areas namely social-media facilitation, internet shopping and reservation / booking etc. has created a powerful economy while enabling borderless exchange of information. The Internet, computers, cell phones and other forms of technology have revolutionized every aspect of human life over these years (Holt, Fitzgerald, Bossler, Chee, & Ng, 2016). On top of this, the ongoing COVID-19 brings blessing globally for service-providers meeting the high-rising market-demands for electronic communications including working from home, banking, shopping, obtaining news and entertaining ourselves (Rahman, 2021b).

These advancements have created huge opportunities committing various forms of crime. These online crimes are referred to as cybercrime (Furnell, 2003; Jain et al., 2016). Thus, it is reasonable to view the Cybercrime as a large umbrella term that encompasses computer-assisted crime in which criminals use computer and technology in a supporting role such as the use of a computer to send harassing messages.

Today's world is a place where real life and using-online are becoming increasingly indistinguishable from each other. Therefore, the widespread access points for cybercrime will continue to grow with the evolution of technology and organizational transformation country-wise where United Arab Emirates (UAE) is no exception. Accordingly, commenting on the "Fight Fraud" campaign, H.E. Abdulaziz Al-Ghurair, Chairman of UAE Banks Federation, recently reminded the UAE that the threat of financial fraud has only increased in a world transformed by the Covid-19 (Gulf, 2021). These progressions have created myriad opportunities for attackers to commit various forms of cybercrime. It occurs because the perpetrators use special knowledge of cyberspace (Furnell, 2003), which means any activities associated with internet and diverse-internet culture. On risk-magnitude perspective, cybercrime can be a low-risk crime, however; managing it effectively can deliver huge payoffs.

These are common *scenarios* of risk-factors associated with today's technology-facilitation in the globe without boundaries. It is severe in magnitudes in countries where the UAE has become a major target because of its continuation of increased economic activities (Al Neaimi, Ranginya, & Lutaaya, 2015). It has increased the usages of internet-services in the UAE (Basamh, Qudaih, & Ibrahim, 2014). Another study shows that over past-years, hackers stole data relates to ATM and credit cards from processing companies and adjusted available balances on these accounts (Hasbini, 2014). The number of the complaints is growing faster in the UAE-economy. Perceived-risk factors in digital-banking have further increased globally during the COVID-19.

Addressing these issues in digital arena, the UAE is not out of controlled by laws. But it needs a framework that can ensure effective communications on cyber-security defense within and outside its agencies. *Particularly*, it needs *piecemeal* approach in practice where approach for one department may vary from approach for another department. Along with raising customer's awareness about risky online-behaviors, tech-users need to put into own efforts underpinning the awareness.

Thus, besides having cybercrime-law in place, this study takes on the challenges to layout the foundations of a proposal, named *Akim's Model-2021*. It is a piecemeal approach along with tech-user's awareness & own-efforts for protection where we use Theory of Consumer Choices & Behaviors to justify the model. This study further carries-out welfare analysis of the proposal country-wise such as UAE in aim to attract lawmakers' attentions for addressing cybercrime problem in the modern-world.

2. LITERATURE REVIEW

The cybercrime is no new in today's technology-driven world. Like in countries, the national security awareness campaign was first launched in the UAE in November of 2007 (Al Neaimi et al., 2015). A survey data-statistics based study reported that in year 2010, many users lost their UAE bank savings through internet-fraud (Hasbini, 2014). Over the years, hackers stole data relates to ATM cards and credit cards from processing companies and adjusted available balances on these accounts (Al Neaimi et al., 2015; Hasbini, 2014). *Later*, these hackers distributed these cards to other hackers for targeting countries to withdraw large volumes of cash (Al Neaimi, Ranginya, & Lutaaya, 2014).

The risk of using digital-banking has further increased globally during COVID-19. On marginalizing the *dilemma*, a distinctive policy-proposal, known as Akim's model in literature (Rahman, 2018) is well recognized. Based on the model, it expects that the Voluntary Insurance (VI) will be a new-product in digital-banking-services. Besides Policy-practitioners globally have well recognized the proposal. Under the proposed VI-policy, either bank or third-party can supply the services and accountholders will bear the insurance-premium (Rahman, 2018). Thus, the proposed VI, in financial institutions in the UAE can be instrumental addressing the perceived-risks or possibilities of fraud in digital-banking.

The United National Development Program (UNDP) Report of 2012 reveals that there are huge potentials in the Middle East to build strong e-government portals that can enhance digital communication and reduce operational costs up to 95 percent (Barrett, 2018). This transformation into technology-driven smart cities or nations requires cooperation, coordination and commitment of all stakeholders and deployment of the right set of skills and infrastructure. Otherwise, it can open path for criminals. Thus, it causes cyber-threats, which are already at an exponential rate in the UAE (Dubai Electronic Security Center, 2017).

All this creates a demand among rational policymakers for cost-perspective analysis of electronic crime & abuses, which was missing until now. So, it fills the gap in relevant literature. This study therefore sets out to use Welfare Analysis for assessing probable costs of cybercrime in world-economy country-wise such as the UAE-economy, which can fill the gap in the literature. It further proposes policy-model, known as "Akim Model-2021" underpinning Theory of Consumer Choices & Behaviors, besides having cybercrime-law in place.

2.1. Why the UAE?

There has been a rapid escalation and intensification of cybercrime activities originating and targeting the Middle East and North Africa (MENA) region (Dubai Electronic Security Center, 2017). Such activities are financially, politically, and ideologically motivated (Hasbini, 2014). In MENA region, the UAE is situated in the Southeast of the Arabian Peninsula, bordering Oman and Saudi Arabia. The UAE is a federation of seven emirates -

Abu Dhabi, Dubai, Sharjah, Ajman, Umm Al-Quwain, Fujairah, and Ras Al Khaimah where Abu Dhabi is the capital city, which is the largest and wealthiest emirate.

Since after forming the Federation, the UAE has developed rapidly and noted for its modern infrastructure, international events and status as a trade and transport hub (Kshetri, 2013). The city of Dubai has also diversified into the exhibitions, events, ICT, re-export, and financial sectors. Taking advantages of its position near the head of the Gulf, it has combined its historical reputation as a regional entre-port. Dubai has developed luxury hotels, large port facilities and a range of free trade zones to attract both manufacturing and services industries.

As of 2018, the UAE-population of 10.4 million depends on its expatriate workforce that made up about 88% of the population. The UAE government has increased spending on job creation and infrastructure expansion including preparations for hosting the upcoming world expo in Dubai (Jain et al., 2016). Also, the UAE is opening utilities to greater private sector involvement and has created free trade zones across the country for attracting foreign investors (DFAT, 2021). Over the years the UAE has built its National Innovation Strategy to become the leading innovation nation. It has begun its journey by defining the word "innovation" in multi-faucets. They are a) the desire of individuals, private institutions, and government to generate creative ideas b) innovative products & services that improve quality of life and c) promote economic growth and increase competitiveness (Chandra, Sharma, & Liaqat, 2019). These strategies have focused on the development of smart cities, updating software and applications of using disruptive method such as nanotechnology and artificial intelligence by ensuring a swift implementation of technology-cross various industries (Chandra et al., 2019).

Transformation into a smart nation requires cooperation, coordination and commitment of all stakeholders and deployment of the right set of skills and infrastructure. These can help ensuring security no matter what country or society we talk about. It is no overstated that possible "glitches" are minimized but not eliminated. Thus, authority should consider security risks at hand in the form of smart-security and cyber-security policies to Dubai's current city and grid infrastructure. So, today's humankind or societies need e-security policy adoption for the protection of a truly modern and technologically advanced city.

All these progressions in multi-faucets and continuation of high-rise economic growth in the UAE, particularly Dubai becomes a global village where social engagement will boom further over the Internet. All these make the UAE to be in further danger on possibilities of cybercrime or cyber-attacks than that in any other smart cities in the globe.

With these technological & economic progressions, the UAE has been suffering with the issue of cybercrime, despites the fact that the UAE has cybercrime-law in place (Creesey & Nayfeh, 2012; Hasbini, 2014). Figure 1 shows that thru debit & credit cards fraud, the accumulated amount of monetary loss was 3861 dirhams, which was the highest among seven categories of financial fraud in the UAE in year 2017. Figure 1 further shows that online purchase fraud amount was the lowest. On cybercrime type, Figure 2 shows that malware infected 53% electronic devices in year 2017.

Figure 2 further shows that defaulted technical support was 24% in the same year. However, since the UAE has the highest number of internet users and since Dubai is the world's business hub (University of Birmingham Dubai, 2021), which will require highest technological usage as years ahead.

For prompt broader involvement of stakeholders within and beyond are needed for ensuring effectiveness & efficiency of cyber-security defense efforts globally. However, independent efforts, most authorities' country-wise now have own cybercrime prevention acts, which have caused inefficiency of the laws in practice. In absence of a broader involvement of parties domestically and as well as globally, the cybercrime impact is getting worse in terms of financial & social costs (DFAT, 2021; University of Birmingham Dubai, 2021).

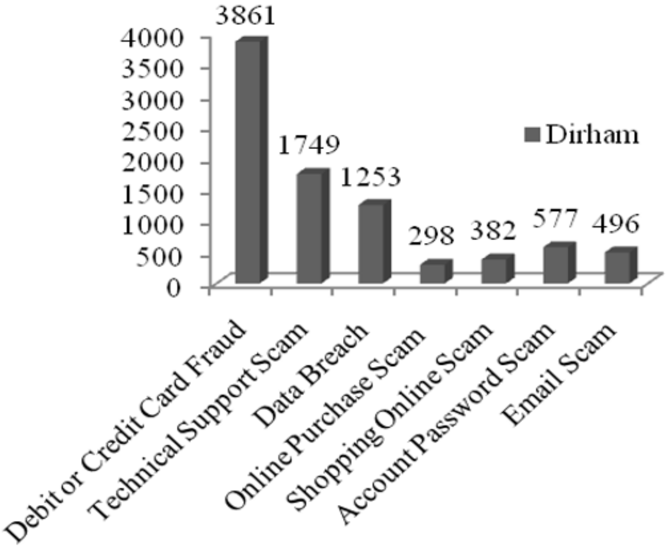

Figure 1. Highest monetary loss in the UAE in 2017.
Source: Naqvi (2018).

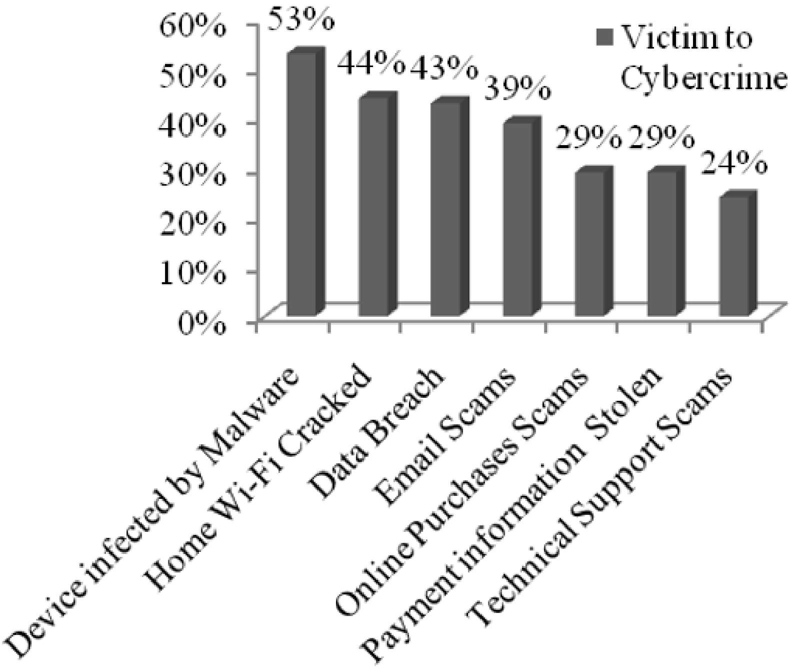

Figure 2. Cybercrime experiences in the UAE in 2017.
Source: Naqvi (2018).

2.2. Types of Cybercrime - What is it and how does it Happen in Reality?

Cybercrime is criminal activity that either targets or uses a computer, a computer network, or a network-device. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money with the cost or damages of someone else. In general individuals or organizations conduct Cybercrime. In most cases, cybercriminals are organized. They use advanced techniques and are highly technically skilled. Others are novice hackers. Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal as we see in today's technology world.

2.2.1. Categories and Types of Cybercrime

There are two distinct categories of Cybercrimes. They are :

1. Cyber-trespass (e.g., unauthorized system access).
2. Cyber-deception / theft (e.g., identity theft, online fraud, digital piracy).
3. Cyber-porn/obscenity (e.g., child sexual exploitation materials).
4. Cyber-violence (e.g., cyber stalking; cyber terrorism) (Holt, Bossler, Kathryn, & Spellar, 2017; Walls, 2001).

2.2.2. Diverse Types of Cybercrime

a. Email and internet fraud.

b. Identity fraud (where personal information is stolen and used).

c. Theft of financial or card payment data.

d. Theft and sale of corporate data.

e. Cyber extortion (demanding money to prevent a threatened attack).

f. Ransom ware attacks (a type of cyber extortion).

g. Crypto jacking (where hackers mine crypto currency using resources they do not own).

h. Cyber espionage (where hackers access government or company data).

The US Department of Justice recognizes a third category of cybercrime which is where a computer is used as an accessory to commit the crime. An example of this is using a computer to store stolen data. So, the US has signed the *European Convention of Cybercrime*. It casts a wide net and there are malicious computer-related crimes which it considers cybercrime. For example

a. Illegally intercepting or stealing data.

b. Interfering with systems in a way that compromises a network.

c. Infringing copyright.

d. Illegal gambling.

e. Selling illegal items online.

f. Soliciting, producing, or having child pornography.

Cybercriminals may infect computers with viruses and malware to damage devices or stop them working. They may also use malware to cut or steal data. Cybercrime can stop users using a machine or network and prevent a business supplying a software service, which is known as Denial-of-Service (DoS) attack (Cybersecurity & Infrastructure, 2019).

Cybercrime that *uses* computers to commit other crimes may involve using computers or networks to spread malware, illegal information, or illegal images. Sometimes cybercriminals conduct both categories of cybercrime at once. They may target computers with viruses first. Then, use them to spread malware to other machines or throughout a network. Cybercriminals may also conduct what is known as a Distributed-Denial-of-Service (DDos) attack. This is like a DoS attack, but cybercriminals use compromised computers to carry it out in general.

2.2.3. How does it Happen?

In this subsection, we look at famous examples of diverse types of cybercrime-attack used by cybercriminals. It can be helpful understanding what counts as cybercrime.

2.2.3.1. Malware Attacks

A malware-attack is where a computer system or network becomes infected with a computer virus or other type of malware. A computer compromised by malware, which cybercriminals could use for different purposes. These include stealing confidential data, using the computer to conduct other criminal acts, or causing damage to data.

A famous example of a malware attack is the WannaCry ransom-ware attack, a global cybercrime committed in May 2017 (Kaspersky, 2017). Ransomware is a type of malware used to extort money by holding the victim's data or device to ransom. WannaCry is a type of ransomware which targeted vulnerability in computers running Microsoft Windows. When the WannaCry ransom-ware attack hit, 230,000 computers were affected across 150 countries. Users were locked out of their files and sent a message demanding that they pay a Bit Coin ransom to regain access. Worldwide, the WannaCry cybercrime has caused approximately $4 billion in financial losses.

2.2.3.2. Phishing

A phishing campaign is when spam emails or other forms of communication send a message, with the intention of tricking recipients into doing something that undermines their security or the security of the organization they work for. Phishing campaign messages may have infected attachments or links to malicious sites. Or they may ask the receiver to respond with confidential information

A famous example of a phishing fraud from 2018 was one which took place over the World Cup. According to reports by *Inc*, the World Cup phishing fraud involved emails sent to football fans. These spam emails tried to entice fans with fake free trips to Moscow, where the World Cup was going on. People who opened and clicked on the links contained in these emails had their personal data stolen.

Another type of phishing campaign is known as spear-phishing. These are targeted phishing campaigns which try to trick specific individuals into jeopardizing the security of the organization they work for. Unlike mass phishing campaigns, which are very general in style, spear-phishing messages typically crafted to look like messages from a trusted source. For example, they look like they have come from the Chief Executive Officer (CEO) or the Information Technology (IT) manager. They may not have any visual clues that they are fakes.

2.2.3.3. Distributed Dos Attacks

Distributed DoS attacks (DDoS) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected Internet of things (IoT) devices are used to launch DDoS attacks. A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests.

Cybercriminals who are conducting cyber extortion may use the threat of a DDoS attack to demand money. Alternatively, a DDoS may use as a distraction tactic while other type of cybercrime takes place. An example of this type of attack is the 2017 DDoS attack on the UK National Lottery website. This brought the lottery's website and mobile app offline, preventing UK citizens from playing.

2.3. Hidden Costs of Cybercrime

Besides damages intellectual-property and monetary-assets, the most overlooked costs of cybercrime come from damages of company performance. This cost can be in multi-faucets particularly financial costs and workhours lost after a cyber-incident. The report further explored the hidden costs, and the lasting impact & damages cybercrime can have on an organization (Kaspersky, 2017).

Cost-incurred from anticipation – Organizations or firm even individuals very often buy or subscribe software such as antivirus software, insurance, and compliance with agreement,

System Downtime – Downtime is a common experience of organizations or firm. The assessed cost of downtime varies from organization to organization corresponding to incidents.

Reduced Efficiency – As a result of system downtime, organizations of firm lose time, which can reduce efficiency.

Incidence Response Costs – In reality, most organizations require adequate time to move from discovery of an incident to remediation. Security incidents are manageable in-house. But major incidents can often require outside consults, which can be expensive.

Brand and Reputation Damage – It can damage external image of the brand of a firm or organization. It can cause a reduction of public sector revenue.

2.4. Policy-options: Awareness & Own-effort of Tech-user, Besides Nation's Cybercrime-law

Theoretical Background: Consumer choice and utility maximization

The progression of digital technologies has been changing economic activities in today's world where cybercrime is not ignorable. The digital progression has also attracted more criminals for monetary benefits. In this process by-and-large a cyber-criminal or attacker extracts an economic payoff by hacking a system of value to a victim and then ask for a ransom to not undermine that value. If these crimes are not properly manageable, they could significantly reduce overall social-welfare received from technology-progressions or increase social-cost of human-society in the 21st Century *Era*.

Thus, studying cybercrimes from economics perspective is important for two reasons (Becker, 1968). *First*, understanding the benefits & costs to the person committing the crime can help on decision committing the crime, which leads to analysis of best approach to limit this crime, given a certain number of resources. *Secondly*, understanding the social costs of a crime can help to decide a socially efficient level of resources that should deploy against it.

Since the 21st Century humankind prefers democratic environment over dictatorships country-wise (Rahman, 2021c) and since society is a formation of all characteristics of people & its behaviors, policy-design goal for a society is not always to cut a crime. Rather, it is for deciding the number of crime and which criminal-behavior should tolerate. This is because reducing the number of crimes to *zero* does not aligns with social interest. This is because

a) Probable economic cost of cutting the crime could be higher than its harms to society.

b) Preference based on this cost-benefit assessment can ease sharpening and ensuring individual's own responsibility. Thus, tech-user has own responsibilities on awareness and accordingly investing efforts in aim to protect the tech-user-self from bad activities out there such as rape-crime or cybercrime.

Since cybercrime is in multi-faceted and a complicated issue, we take freedom and cast a simple example for better understanding why a society decides "how much and which behavior" should we tolerate in society (Rahman, 2021c). Suppose Lavina, a female-gender, wants to see rape-free human-society. To fulfill Lavina's demand, authority needs to assign law-enforcement wherever male & female are together. Meeting Lavina's demand can be very expansive, and it can undermine Lavina's own efforts to protect herself. However, it is an essential part for a human growing up for survival no matter what culture or society we are in. It is obvious Lavina's social background, education level and age can be instrumental in her awareness & own-efforts for her own-safety besides having nation's Rape Law in place.

This *scenario* in cybercrime cases raises question: what numbers of offenses should a society allow and what number offenders should go unpunished?

The method we use is for formulating a measure of the social loss from offenses and finds those expenditures of resources and punishments that minimize this loss. The best amount of enforcement as shown depends on, among other things, a) the cost of catching & convicting offenders b) the nature of punishments—for example, whether they are fines or prison terms—and c) the responses of offenders to changes in enforcement.

So, this study proposes *piecemeal* approach or separately considering each issue of cybercrime under general provision of cybercrime where a proposal of newly establishing Agency or Commission can be instrumental for effective outcome. Under its administration, responsibilities can be broken down based on type of cybercrime in piecemeal choice. Outcome under this setup can be effective where attacker gets punished, and tech-user feels eased with training & guidance on awareness and protecting self from probable dangers. Otherwise, the current system may often fail unless they are broken into pieces. In this setup, besides having cybercrime law in place, tech-user's approach to a task or situation will be the way the tech-user deals with it or think about it where tech-user's awareness and self-effort can play significantly.

2.4.1. Assumptions

In our model, three parties namely a) Tech-user b) Attacker and c) Policymaker are involved. Besides benefit-cost assessment, an attacker learns about tech-user's level of defense, which serves as a sample for the attackers to learn about that of entire tech-users-population. Therefore, if tech-user is under attack with lacks defense, the attacker will feel encouraged to continue. On the other hand, if tech-user is well-defended, the attacker will feel discouraged to continue.

Attacker in some cases receives ransom from tech-user or defender. Despite the fact, this study ignores attacker's welfare including such redistributed wealth as part of social welfare. Thus, in this study assumes the following

a) There is no relevant other factor, except risk-factor of cybercrime consequence, which can make changes.

b) Here a rational tech-user's preferences of self-defense depend on tech-user's understanding of severity of the risk-factor.

c) These preferences are stable, total efforts and transitive for maximizing utility of risk-protective choices.

2.4.2. Awareness & Own-efforts of Tech-users under Theory of Consumer Choices & Behaviors

It is now well recognized that perceived-risk factor plays an influential role in tech-user's decision (Rahman, 2018) . It is no different when it come awareness and self-efforts for being on safe-side in case of risk-factor such as cybercrime (Rahman, 2021a). It is palatable to assume that on rationality perspective, the tech-user is risk-averse, *i.e.*, the tech-user prefers certainty over uncertainty when it comes protecting tech-user from the danger out there. Figure 3 illustrates the risk preferences of a risk-averse for a rational and conscious tech-user who is concerned cybercrime.

Tech-user's actual benefit or utility that the tech-user receives from awareness & self-efforts will never fall on the line Total Utility (TU) but on the chord (the bold line) as shown in Figure 3**.** The point X_g, in Figure 3 stands for probable outcomes of services (X). Here outcome = f (cybercrime laws in place and tech-user's awareness & own-preventive-effort). That ensures a necessity of joint-efforts individual from tech-user or government-cybercrime-law on effectively preventing crime. So, tech-user may use certain level of X.

Here tech-user's awareness & self-effort (AE) = f (age, education level, experience). Thus, outcome of cybercrime prevention depends on a) strength of cybercrime laws and b) tech-user's awareness & own preventive-effort. It means the outcome of service-on-security depends on full use of cybercrime law, tech-user's own awareness & self-effort, which can ensure the highest level of security. Thus, it may cost higher for ensuring highest level of security. Any changes to these services-on-security may risk tech-user to be a victim. It may cost lower but it can put tech-user at risk.

In this setup, X_g in Figure 3 stands for services derived from supportive-factors such as cybercrime-law, tech-user's awareness & own effort, which produce the highest outcome "secured from cybercrime." X_f stands for service-on-security derived from cybercrime-law where $X_g > X_f$. In case of X_f, (where X_f indicates cybercrime law in place) tech-user enjoys lower cost, which may produce outcome "getting attacked." If there exists a level of consequences, a tech-user may give a try to use X_g units of service-on-security X, the utility that this tech-user receives will lie somewhere on the chord (the bold line). The chord is the Expected Utility (EU) of using service-on-security X, which lies in the concavity of the curve. This is because it is the average probability that the defender will use service-on-security X or not where X stands for the combination of cybercrime-law and tech-user's awareness & own effort. As a result, the tech-user will never receive TU (X_a) but EU (X_a).

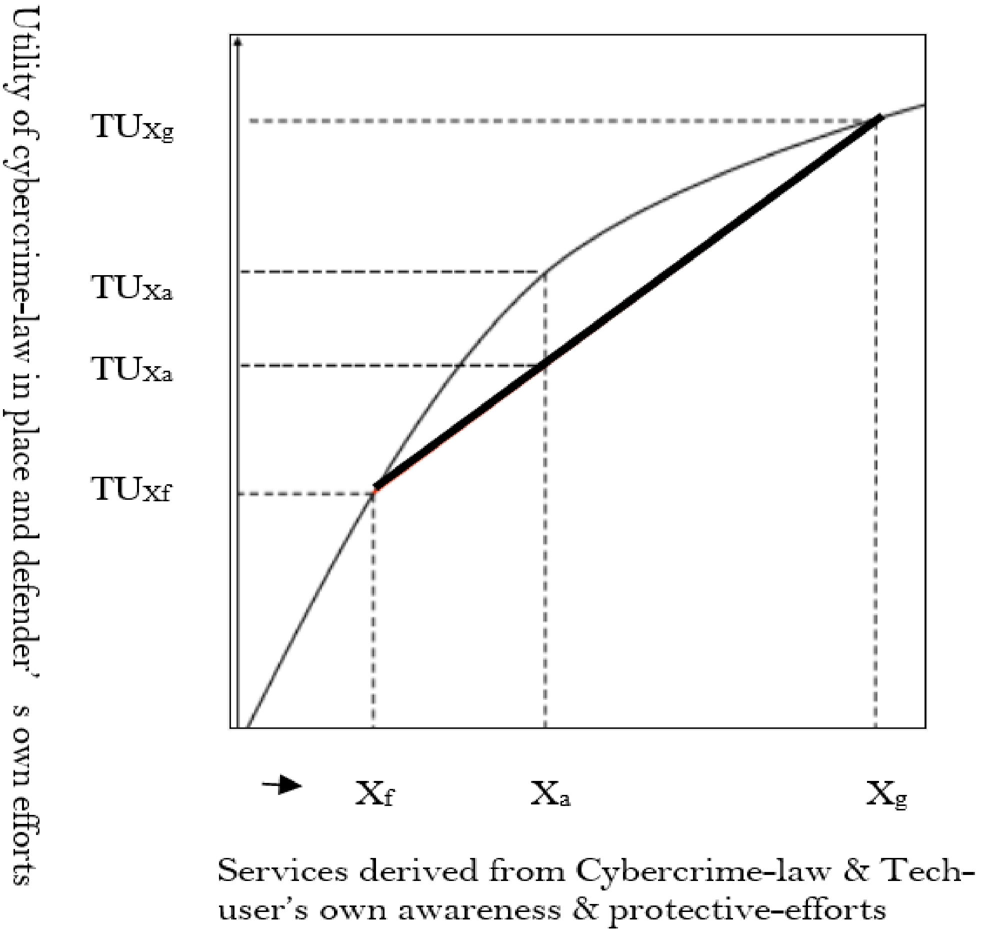
Utility of cybercrime-law in place and defender' s own efforts
TUXg
TUXa
TUXa
TUXf
Xf
Xa
Xg
Services derived from Cybercrime-law & Tech-user's own awareness & protective-efforts

Figure 3. Cybercrime-risk aversion *scenario* that has laws in place along with Tech-user's awareness & own-effort.

2.5. Policy Adoption: Awareness & Own-Effort along with Cybercrime-Law in Place Country-Wise

In aim to examine benefits of investing tech-user's time for awareness & self-efforts besides having cybercrime-law in place for protecting tech-user, we design this section as follows

It is important for tech-user as well as government to get full information about the economic benefits of adopting cybercrime-law and encouraging for tech-user's awareness & own-effort for ensuing secure technology usages globally country-wise.

2.5.1. Approaches other than Cybercrime-Law: Policy Guidance

Since cybercrime is a global problem country-wise, tech-users' behaviors are the key facing the perceived-risk of cybercrime besides having cybercrime-law in place country-wise. So, this section advances analyzing probable approaches besides cybercrime-law in place, which can be instrumental addressing today's cybercrime effectively country-wise.

Evidence suggests that most governments country-wise have acknowledged the problem of cybercrime by having preventive laws, mostly known Cybercrime Law. However, the UAE, like countries have done little engaging tech-users for awareness & own-effort protecting tech-usage. So that people in the UAE can be familiar with cybercrime & consequences and can recognize the importance of preventive-measures from the tech-user's side. It can also supply cyber-security awareness training for employees and develop prevention & response plans.

2.5.2. Guiding Tech-Users on Required Behaviors Facing Perceived-Risk of Cybercrime

In today's world, people are mostly driven by their own benefits in multi-faucets such as financial, feeling good, self-recognition, self-pride etc. In this decision-making process, an individual can be a risk-adverse or risk-taker. Thus, using technology facilitations, the proposed guidance should be in such way so that both groups can get help aiming to facing perceived risk of cybercrime.

Risk-benefit analyses can be useful in delivering message for convincing tech-users on avoiding risk. Most human make decisions subconsciously. So, by thinking about risks and benefits of tech-user's actions, the tech-user can make better decisions in choices. On own-efforts aspect, few options the tech-user can choose. They are as follows

a. Backing up data periodically.
b. Getting protection against malware.
c. Being smart with password and making Changes periodically.
d. Review self-data before going for IT security solution.
e. Being aware about phishers.
f. Buying voluntary insurance, particularly for digital banking services.

2.5.3. Emphasizing Factors That Increase Tech-User's Fondness on Being Safe-Side

In human-society globally country-wise, it is not overstated that using coercive measures such as threats, force, shouting etc. can have a backfire effect rather than enhancing effective public engagement on common issue such as the current crisis (Rahman, 2021c). However, when authorities manage the procedure and explain the importance to follow lockdown-laws, have-on-mask etc. and authorities supply regular updates about their actions, it increases feelings of the legitimacy of the procedure among casualties (Rahman, 2021c).

2.5.4. Welfare Analysis of the Proposal Underpinning Nation's Cybercrime-Law

Based on the proposal underpinning cybercrime law in place, tech-user's decision on securing tech-usage by setting Marginal Private Cost = Marginal Private Benefit symbolically MPC = MPB in Figure 4. Because of tech-user's inspiration, the market level of tech-user's awareness & own-effort Q_1 and best level is Q^* that are generated underpinning nation's cybercrime-law and government's promotional efforts. Area K stands for net social-gains, which is the outcome of joint-efforts of Govt. and Tech-user's effort.

In Figure 5, area (A+B+C+D+E) is tech-user or defender's surplus. Government spends for cybercrime-law implementation is area (E+B+C+D+F), which is collected from taxpayers. Net loss to UAE is (E+F). Area E reflects a net loss of producer (technology producers) surplus, underutilized resources better business or more selling opportunities. Area F is deadweight loss that is gone.

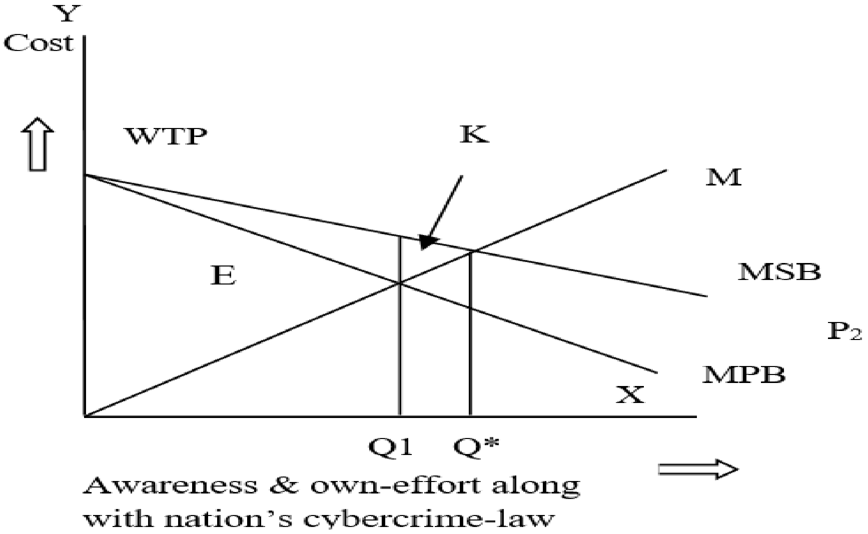

Figure 4. Welfare from awareness & own-effort under cybercrime-law implementation in the UAE.
Note: MPB = Marginal private benefit, MSB = Marginal Social Benefit, WTP = Total willingness to pay and K = Net social gain.

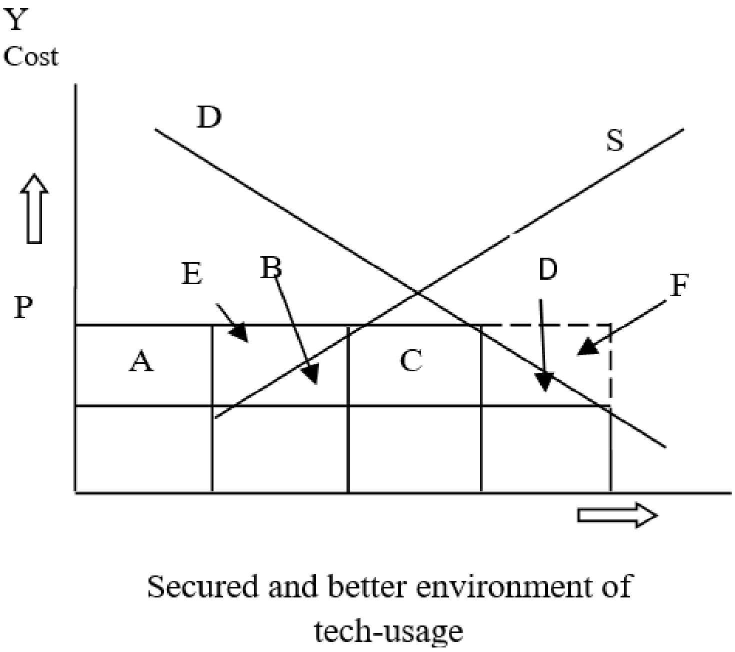

Figure 5. Welfare aspect of secured & better environment of tech-usage.

2.6. Future Study

Since cybercrime is a vast & complicated arena, which may get worse *parallel* to the trends of growing number of tech-users, it requires for taking effective & protective measures now than later. Since the current study is a theoretical one, after data collection from tech-users in different fields, can conduct empirical studies for welfare analysis. Further studies can be conducted on application of Voluntary Insurance in securing digital-banking underpinning Akum's Model (Rahman, 2018). It can further contribute to the understanding, prevention, or correction of criminal behaviors of cybercrime in digital-banking services. *Lastly*, an opinion-survey study can be conducted on how the tech-users feel about the proposal "awareness & own efforts" besides having cybercrime-law in place country-wise such as the UAE.

3. CONCLUSION

Today's technology-driven world is counted more than ever before where the United Arab Emirates (UAE) society is no different in the globe. Thus, here decision-factors convenience and cost-effectiveness have led individuals, organizations, agencies, or businesses welcoming ICT-facilitations for using in multi-folds. As a result, meeting society-needs, sectors including service-sector like banking is in the process modernization. Here customers compete for comparative time-saving-option(s) for marginalizing its operating costs. With the increase of data-usage, number of tech-users and devices, cybercrime has been on rise, which is all-time high ever since. Only until recent times, we are coming across increased stories about the data-breach and cybercriminal activities. Addressing the issue, like in other countries, the UAE is not out of controlled by laws. Since human society is a formation of all characteristics of people & its behaviors, the law for its society is not always to cut a crime. This is because reducing amount of crime to *zero* may not necessarily be aligned with social interest. It can increase probable economic cost cutting the crime, which could be higher than its harms to society.

But it needs a framework that can ensure effective communications on cyber-security defense within and outside its agencies. *Particularly*, it needs *piecemeal* approach in practice where approach for one department may vary from approach for anther department. Raising tech-user's awareness about risky online behaviors and accordingly tech-users need to put own-efforts underpinning the awareness about the crime and probable options available to the tech-users. Thus, besides having cybercrime-law in place, this study takes on the challenges to layout the foundations, named *Akim's Mode-2021*, of *piecemeal* approach along with tech-user's awareness & own-efforts for protection using Behavior Theory of Consumer Choices. It further carries-out welfare analysis of the cost's country-wise such as the UAE in aim to attract leaderships' attentions for addressing cybercrime in a *piecemeal* approach.

Findings show that tech-user's actual benefit or utility that a tech-user receives from awareness & self-efforts along with cybercrime-law in place is not exactly equal to its total utility. Here certain part of utility come from service-on-security derived from cybercrime-law where total utility is greater than utility-received from cybercrime-law. Thus, outcome of cybercrime prevention depends on strength of cybercrime-law and tech-user's awareness & own preventive-effort. It means the outcome of service-on-security depends on a) full use of cybercrime-law b) tech-user's own awareness & self-effort, which can ensure the highest level of security. Thus, it may cost higher for ensuring highest level of security. Any changes to these services may risk being a victim. It may cost lower but it can put the tech-user at risk.

On welfare analysis perspective, the findings show that tech-user's actions including awareness & own-effort, besides government law can create a net social-gain, which significantly depends on tech-users' actions. In this case, tech-users' calculated economic surplus is greater than government's expenses for implementation of the cybercrime-law where the UAE-taxpayers bear the burden. Net loss to the government of the UAE is the sum of deadweight loss plus the net loss to tech-producers because of underutilized resources better business or more selling opportunities.

Since today people move by their own benefits in multi-faucets such as financial, feeling good, self-recognition, self-pride etc. the guidance of tech-users on required behaviors should be in such way so that both government & tech-user can get help aiming to facing perceived-risk of cybercrime. Risk-benefit analyses can be useful in delivering message thru multi-faucets for convincing tech-users on avoiding risk by their own-actions. Furthermore, it can ease sharpening and ensuring individual's own responsibility, which can be the byproduct of the Akim's Model-2021, no matter where tech-users live in the globe country-wise.

REFERENCES

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2014). *A critical analysis of the effectiveness of cyber security defenses in UAE government agencies.* Paper presented at the Proceedings of the International Conference on Information Security and Cyber Forensics, Kuala Terengganu, Malaysia, SDIWC, pp. 1-8.

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates. *International Journal of Cyber-Security and Digital Forensics, 4*(1), 290-301.Available at: https://doi.org/10.17781/p001502.

Barrett, M. (2018). Framework for improving critical infrastructure cybersecurity version 1.1. *NIST Cybersecurity Framework*, 1-55.Available at: https://doi.org/10.6028/NIST.CSWP.04162018.

Basamh, S. S., Qudaih, H., & Ibrahim, J. B. (2014). An overview on cyber security awareness in Muslim countries. *International Journal of Information and Communication Technology Research, 4*(1), 1-4.

Becker, G. S. (1968). Crime and punishment: An economic approach. In the economic dimensions of crime (pp. 13-68). London: Palgrave Macmillan.

Chandra, G. R., Sharma, B. K., & Liaqat, I. A. (2019). UAE's strategy towards most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering, 8*(12), 2803-2809.Available at: https://doi.org/10.35940/ijitee.l3022.1081219.

Creesey, R., & Nayfeh, M. (2012). *Cyber capability in the Middle East: Seizing opportunity while managing risk in digital age*: Booz Allen Hamilton.

Cybersecurity, & Infrastructure, S. A. (2019). Security tip (ST04-015): Understanding denial-of-service attacks. Last revised 20 November 2019. Retrieved from: https://us-cert.cisa.gov/ncas/tips/ST04-015.

DFAT. (2021). United Arab Emirates country brief. Department of foreign affairs and trade, Australian government. Retrieved from: https://www.dfat.gov.au/geo/united-arab-emirates/united-arab-emirates-country-brief.

Dubai Electronic Security Center. (2017). *Establishing Dubai as a global leader in innovation, safety, and security. Dubai cyber security strategy.* Dubai: Government of Dubai.

Furnell, S. (2003). *Cybercrime: Vandalizing the information society. The lecture notes in computer science book series.* Paper presented at the International Conference on web Engineering.

Gulf, N. (2021). How to protect yourself against the threat of cybercrime: UBF's fraud awareness campaign looks to educate customers on cyber fraud risks. Published: Retrieved from: https://gulfnews.com/uae/how-to-protect-yourself-against-the-threat-of-cybercrime-1.1625033096265.

Hasbini, M. A. (2014). The rise of cybercrime in Dubai and UAE. Retrieved from: http://securelist.com/blog/research/63682/the-rise-of-cybercrime-in-dubai-and-uae.

Holt, T. J., Fitzgerald, S., Bossler, A. M., Chee, G., & Ng, E. (2016). Assessing the risk factors of cyber and mobile phone bullying victimization in a nationally representative sample of Singapore youth. *International Journal of Offender Therapy and Comparative Criminology, 60*(5), 598-615.Available at: https://doi.org/10.1177/0306624x14554852.

Holt, T. J., Bossler, A., Kathryn, C., & Spellar, S. (2017). Cybercrime and digital forensics - an introduction. Routledge. Retrieved from: https://www.routledge.com/Cybercrime-and-Digital-Forensics-An-Introduction/Holt-Bossler-Seigfried-Spellar/p/book/9781138238732.

Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., & Kumar, R. (2016). Social engineering: Hacking a human being through technology. *IOSR Journal of Computer Engineering, 18*(5), 94-100.

Kaspersky. (2017). What was the WannaCry ransom-ware attack? Retrieved from: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

Kshetri, N. (2013). Cybercrime and cybersecurity in the Middle East and North African economies. In cybercrime and cybersecurity in the Global South (pp. 119-134). London: Palgrave Macmillan.

Naqvi, R. (2018). Nearly Dh 4 billion lost in the UAE to cybercrime in 2017. Retrieved from: https://gulfnews.com/technology/nearly-dh-4-billion-lost-in-the-uae-to-cybercrime-in-2017-1.1541674889300.

Rahman, A. M. (2018). Voluntary insurance for ensuring risk-free on-the-go banking services in market competition: A proposal for Bangladesh. *The Journal of Asian Finance, Economics and Business, 5*(1), 17-27.

Rahman, A. M. (2021c). Have-on-mask and maintain-physical-distance: Are they the outcome of lockdown-laws in Corona-Virus Crisis Country-Wise. *Journal of Economics and Behavioral Studies, 13*(4), 31-40.Available at: https://doi.org/10.22610/jebs.v13i4(j).3198.

Rahman, A. (2021a). CO2 emission from brickfields in Bangladesh: Can ethical responsibility by doing reduce level of emission? *Athens Journal of Social Sciences, 9*(3), 255-272.Available at: https://doi.org/10.30958/ajss.9-3-3.

Rahman, A. (2021b). Open question to humankind country-wise wearing-mask and maintaining-distance: Are they the outcome of lockdown-law? Retrieved from: https://www.researchgate.net/publication/354219163_Open_Question_to_Humankind_Country-wise_Wearing-mask_and_Maintaining-distance_Are_They_the_Outcome_of_Lockdown-law.

University of Birmingham Dubai. (2021). The world's business hub. Retrieved from: https://www.birmingham.ac.uk/dubai/dynamic-dubai/the-world's-business-hub.aspx.

Walls. (2001). Typology of cybercrime cybertrespass. Retrieved from: https://www.coursehero.com/file/p3os0oo/Walls-2001-typology-of-cybercrime-Cybertrespass-Crossing-boundaries-into-other/.