Information Management and Business Review (ISSN 2220-3796)
Vol. 13, No. 2, pp. 43-55, June 2021

Social-Costs Perspective Impacts of Cybercrime in World-Economy, Country-Wise: Policy-Guidance under Piecemeal Approach

Akim M. Rahman[1] & Saadi Islam[2]
[1]Dept of Economics, Canadian University of Bangladesh, Bangladesh
[2]Public Relations, American International University-Bangladesh (AIUB), Bangladesh
akim_rahman@hotmail.com, rahman.19@osu.edu, saadi.islam1990@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 costs. It has resulted in huge data usages, a high number of users & devices, which has attracted criminals for taking advantage, which is called cybercrime. Addressing cybercrime, the UAE, like many countries, is not out of control 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 a *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 are needed to invest their efforts. This study has laid out the foundation of the proposal, *Akim's Model-2021*, using the 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 largely depends on tech user's 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: *Cybercrime, piecemeal approach, sense of responsibility, awareness & own-effort, perceived risks, theory of consumer choice & behaviors.*

1. Introduction

Today's human race lives in world of business mentality with a technology-driven modern lifestyle. In this lifestyle, services are carried out in multi-faucets, competitive and rational manner (Rahman, 2018). Time values in this technology-driven world are counted more than ever before no matter what society or country we talk about. The United Arab Emirates (UAE) society is no different in the globe. As a result, meeting society's needs, many sectors including service-sector like banking has been modernized (Rahman, 2018). Here tech-users compete for comparative time-saving-option(s) marginalizing its operating costs. This continued development of ICT utilization in other areas namely social-media facilitation, internet shopping and reservation, etc. have created a powerful economy while enabling the 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 et al., 2016). On top of this, the ongoing COVID-19 brings blessing globally for service providers who provide services meeting the high-rising market demands for electronic communications in multi-faucets including working from home, banking, shopping, obtaining news and entertaining ourselves, etc (Rahman, 2021b).

However, these advancements have created huge opportunities for committing various forms of crime (Cybersecurity & Infrasture Security Agency, 2019). These online crimes are referred to as cybercrime (Furnell, 2003; Jain et al., 2016). Cybercrime can therefore be viewed as a large umbrella term that encompasses computer-assisted crime in which computers and technology are used in a supporting role including the use of the computer to send harassing messages. With global cybercrime damages predicted to cost up to $10.5 trillion annually by 2025, not getting caught in the landslide is a matter of taking in the right information and acting on it quickly (Zaharia, 2021). As of 2020 data statistics, Iceland stands first when it comes to cybercrime risk where the UAE positions third in the globe (NordVPN, 2020). In reality, today's world is a place where real life and usages 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 the United Arab Emirates (UAE) is no exception.

Accordingly, comments on the "Fight Fraud" campaign, H.E. Abdulaziz Al-Ghurair, Chairman of UAE Banks Federation (Gulf News, 2021). Recently various sources reminded the UAE that the threat of financial fraud has only increased in a world transformed by Covid-19 (Gulf News, 2021; Cherrayil, 2016). In reality, these progressions and their usages 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 the internet and diverse internet culture. From a risk-magnitude perspective, cybercrime can be a low-risk crime, however; managing it effectively can deliver huge payoffs. These are the common scenarios of risk factors associated with today's technology-facilitated usages in the globe without boundaries. It is severe in magnitudes in some countries where the UAE has become a major target because of its continuation of increased economic activities, tourism, technology and the rise of oil and gas industries (Al Neaimi et al., 2015). These all together have increased usages of internet services in the UAE (Basamh et al., 2014). Another study shows that over the years, hackers stole data related to ATM and credit cards from processing companies and adjusted available balances on these accounts (Hasbini, 2014).

The number of complaints is growing faster in the UAE economy. Digital-banking perceived risk or threat has further increased globally during the Covid-19. Addressing the issues in the digital arena, the UAE is not out of control by laws. But it needs a framework that can ensure effective communications on cyber-security defense within and outside its agencies. Particularly, it needs a piecemeal approach in practice where the approach for one department may vary from the approach for other departments. Along with raising customers' or tech users' awareness about risky online behaviors, tech-users are needed to put their 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, which can be called Akim's Model-2021, a piecemeal approach along with ensuring tech user's awareness & own-efforts for protection using Theory of Consumer Choices & Behaviors. It further carries out welfare analysis of the proposal country-wise such as the UAE intending to attract lawmakers' attention for addressing the cybercrime problem in the modern world. Lastly, this study put forward recommendations for effective policy design country-wise.

2. Literature Review

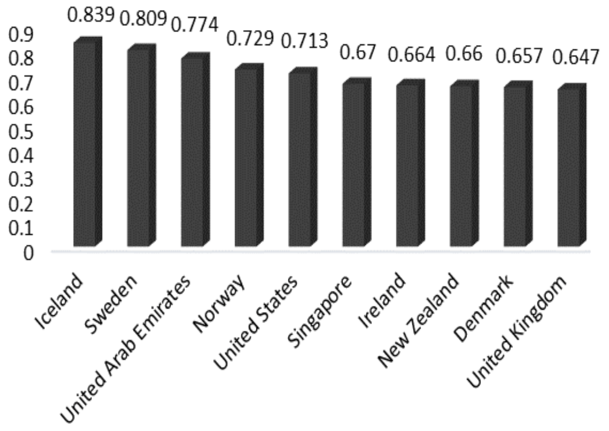
Cybercrime is no new in today's technology-driven world. Like in many countries, the national security awareness campaign was launched in the UAE first in November of 2007 (Al Neaimi et al., 2015). In a study based on survey data statistics, it was reported that in the year 2010, several users lost their UAE bank savings through internet fraud (Hasbini, 2014). Over the years, hackers stole data related to ATMs and credit cards from processing companies and adjusted available balances on these accounts (Hasbini, 2014; Al Neaimi et al., 2015). Later, these cards were distributed to other hackers for targeting countries to withdraw large volumes of cash (Al Neaimi et al., 2015). Digital-banking perceived risk or threat has further increased globally during the Covid-19. On marginalizing the dilemma, a distinctive policy proposal, which is also known as Akim's model was made in literature (Rahman, 2018). Underpinning the model, it is expected that the Voluntary Insurance (VI) will be a new product in digital-banking-services in world-economy country-wise. The proposal has been well recognized by policy practitioners globally. Under the proposed VI policy, either bank or third party can provide the services and account-holders will bear the insurance premium (Rahman, 2018). Thus, the proposed VI, in financial institutions in the UAE can be instrumental in undermining criminal activities in digital-banking services.

It can address the perceived risk of fraud in digital-banking services, which can instrumentally reach the "Cash-less" human society. The 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 up a 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 policy-makers for cost perspective analysis of online/electronic crime & abuses, which was missing until now. Accordingly, it creates a gap in the relevant literature. This study, therefore, sets out to use Welfare Analysis Technique for assessing probable costs of cybercrime country-wise-economy such as the UAE-economy, which can fill the gap in the literature. It further proposes a policy model, which is called "Akim

Model-2021" underpinning the Theory of Consumer Choices & Behaviors, besides having cybercrime law in place. Lastly, this study makes recommendations, which can be helpful in policy design for effective outcomes addressing the perceived risk of cybercrime.

Why the UAE?: There has been an escalation & intensification of cybercrime activities originating in and targeting the Middle East and North Africa (MENA) region (Dubai Electronic Security Center, 2017; Economist Intelligent Unit, 2018)). On the cyber-risk aspect, in Figure 1, the UAE places the 3rd position in the world even though it is not prepared to meet the crisis, Table 1.

Figure 1: Countries with the Highest Cybercrime Risk



Source: Nord VPN, 2020

Table 1: Preparedness on Cyber Security in GCC Countries (20018-19)

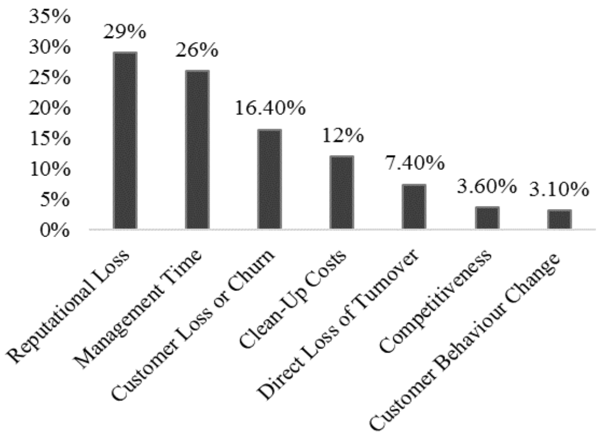
Country	Score 0=High Preparedness 4=Low Preparedness
Qatar	0
Oman	0
UAE	1
Bahrain	2
Saudi Arabia	2
Kuwait	3

Source: Economist Intelligence Unit, 2018

Such activities are financially as well as politically and ideologically motivated (Jain et al., 2016). In the MENA region, the UAE is situated in the Southeast of the Arabian Peninsula, bordering Oman and Saudi Arabia. The UAE is a federation of six emirates - Abu Dhabi, Dubai, Sharjah, Ajman, Umm Al-Quwain, Fujairah and Ras Al Khaimah. The capital city is Abu Dhabi, located in the largest and wealthiest of the seven emirates. Since after forming the Federation, the UAE has been developed rapidly and is now 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 advantage of its position near the head of the Gulf, it has consolidated 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 largely 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 up utilities to greater private sector involvement and has created several 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.

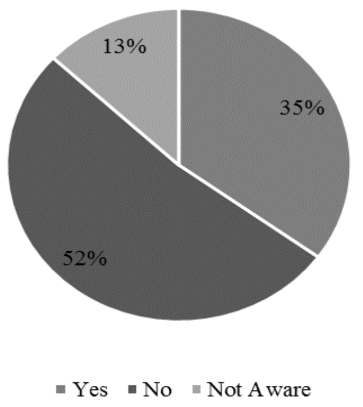
It has begun its journey by defining the word "innovation" in multi-faucets. They are a) the desire of individuals, private institutions and government to generate creative ideas b) innovative products & services that improve quality of life and c) promote economic growth and increase competitiveness (Chandra et al., 2019). These strategies have mainly focused on the development of smart cities, updating software and applications of using disruptive methodology such as nanotechnology, artificial intelligence, etc. by ensuring a swift implementation of technology across 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 ensure security no matter what country or society we talk about. It would not be overstated that possible "glitches" seem to be minimized but not eliminated. Thus authority should consider possible security risks at hand in the form of smart security and cyber-security policies to Dubai's current city and grid infrastructure. Accordingly, an e-security policy needs to be adopted for the protection of a truly modern and technologically advanced city. All these progressions in multi-facets 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 be in more danger of possibilities of cybercrime or cyber-attacks than that in any other smart city in the globe.

Figure 2: The Primary Impact of Cyber Attack in UAE



Source: Grant Thornton, 2017

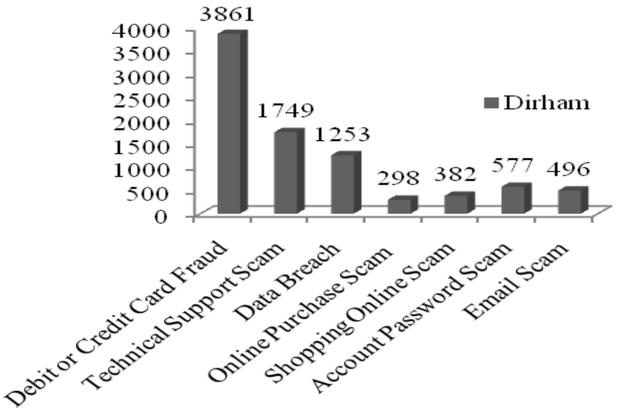
Figure 3: Most Firms Have no Cyber Insurance



Source: Grant Thornton, 2017

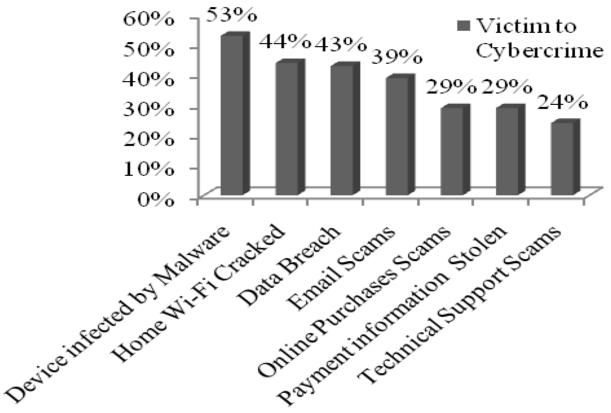
With these technological & economic progressions in multi-faucets, the UAE has been suffering from the issue of cybercrime, even though the UAE has cybercrime-law in place (Hasbini, 2014; Creesey and Nayfeh, 2012). Direct and indirect impact & costs evolved from cybercrime in the UAE are shown in Fig-2 where reputational cost is the highest and cost from customer behavioral changes stands the least. Despite these social costs, besides the cybercrime law in place, Fig - 3 shows that 52 % of business firms in the UAE do not have cybercrime insurance. In an aim to effectively face the perceived risk factors, the government may consider the Voluntary Insurance approach underpinning Akim's Model (Rahman, 2018). In the year 2017, thru debit & credit cards fraud, the accumulated amount of financial loss was 3861 Dirham, which was the highest among seven categories of financial fraud in the UAE, Figure 4 where online purchase scam amount was the lowest.

Figure 4: Highest Financial Loss in the UAE in 2017



Source: Naqvi, 2018

Figure 5: Cybercrime Experience in UAE in 2017



Source: Naqvi, 2018

On cybercrime type, Figure 3 shows that 53% of electronic devices were infected by malware in the year 2017. Figure 5 further shows that 24% of technical supports was scammed in the same year. Since 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 the highest technological usage as years ahead. For prompt broader involvements of stakeholders within and beyond are needed for ensuring effectiveness & efficiency of cyber-security defense efforts. However, independent efforts, most authorities country-wise now have their own cybercrime prevention acts, which has caused inefficiency of the law 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 (University of Birmingham Dubai, 2021; DFAT, 2021).

Types of Cybercrime - What is it and how does it happen in Reality? Cybercrime is an activity of a criminal who either targets or uses a computer, a computer network or a network device. In most cases, cybercrime is committed by cybercriminals to make money at the cost of someone else. It is carried out by individuals or groups. Some of these criminals are organized and use very advanced techniques. Others are novice hackers. Rarely, these criminals aim to damage computers for reasons other than profit. These could be political or personal as we are witnessing in today's modern world.

Categories of Cybercrime: In general, Cybercrimes can be classified into four categories (Holt et al., 2017; Walls, 2001). They are

- Cyber-trespass
- Cyber-deception
- Cyber-porn/obscenity
- Cyber-violence

Types of Cybercrime: Cybercrime types, in general, are as follows (Holt et al., 2017; Walls, 2001).

- Email fraud
- Identity fraud
- Theft of credit-card payment information
- Theft of corporate data statistics or secretly selling corporate data
- Cyber extortion
- Ransomware attacks
- Crypto-jacking
- Cyber espionage

Others: Besides the above types of cybercrime, the US Department of Justice (US DOJ) has recognized another type of cybercrime. It is the type that involves storing data using the computer(s) as an accessory(s) for committing the crime. In an aim to prevent this type of cybercrime, the US Government has signed up with the European Convention on Cybercrime. This type of cybercrime can be identified as follows

- Intercepting Illegally
- Interfering with systems in such-way so that compromise a network
- Infringing copyrights
- Gambling Illegally
- Selling illegal items Online and
- Soliciting, producing or possessing child pornography

Extra Scenario(s) or Way(s) that is considered to be Cybercrime: Cybercriminals may cause damages to devices or computers using viruses and malware in aim to stop them from working. They may also use malware for deleting or stealing information. Using a technique called Denial-of-service (DoS) cybercriminals may try stopping users using a machine or network or prevent a business from providing a software service to its customers (Cyber-security & Infrastructure Security Agency, 2019). Criminals may choose to spread illegal information or illegal images or spread malware using computers or networks. Cybercriminals may also carry out what is known as a Distributed-Denial-of-Service (DDos) attack, which is similar to a DoS attack.

How Do these Happen? With examples of these types of cybercrime attacks are given below for a helpful understanding of what counts as cybercrime.

Malware Attacks: A malware attack is where a computer system or network is infected with a computer virus or malware. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts or causing damage to data. A famous example of a malware attack is the WannaCry ransomware attack, a global cybercrime committed in May 2017 (Kaspersky, 2017).

Phishing: A phishing campaign is when spam emails or other forms of communication are sent messages with the intention of tricking recipients into doing something that undermines their security. It may contain links or attachments, particularly infected ones. It may ask the receiver for a response with confidential information (Kaspersky, 2017). A famous example of a phishing scam from 2018 was the one that took place over the World Cup where messages were sent to football fans. Accordingly, the criminals tried to entice fans with fake free trips to Moscow where the World Cup event was going on.

DDoS-Attack: It is one of the kinds of cybercrime-attack that is used by criminals to bring down the network. This type of attack first took place in 2017 on the UK National Lottery website. This brought down the lottery's website (Kaspersky, 2017).

Hidden Costs of Cybercrime: Besides damages intellectual property and monetary assets, the most overlooked costs of cybercrime come from damages to company performances. This cost can be in multi-faucets particularly financial costs and work-hours lost after a cyber-incident. The report further explored the hidden costs and the lasting impact and damage cybercrime can have on an organization including (Lewis et al., 2020). Figure 2 clearly shows that the UAE faces multi-faucets hidden-cost of cybercrime. They are mainly reputation cost, management time, customer behavior change, etc. Besides these, the following are major components of the hidden cost of cybercrime in the UAE.

Cost-Incurred from Anticipation: Firms even individuals very often buy or subscribe to software such as antivirus software, insurance and compliance with the agreement.

System Downtime: Downtime is a common experience of firms, organizations, etc. The assessed cost of downtime varies from organization to organization on an incident aspect.

Reduced Efficiency: As a result of system downtime, organizations or firm loses time, which can reduce efficiency.

Incidence Response Costs: In reality, most organizations or firms require adequate time to move from the discovery of an incident to remediation. Many security incidents can be managed in-house. But major incidents can often require outside consults, which can be very expensive.

Brand and Reputation Damage: It can damage the external image of the brand of the firm or organization, which can negatively influence its revenue levels, which can hurt the government's tax-revenue levels.

3. Methodology

In an aim to establish the basis of policy guidance under piecemeal-approach, this study uses the Theory of Consumer Choice & Behaviors (Rahman, 2019). It puts forward effective policy-design guidance for leadership country-wise such as the UAE, as well as for tech-user in deciding on its actions to protect own device from cybercrime acts and beyond. Accordingly, in this study, the policy-options assumptions are made. Finally, this study carries out a Welfare Analysis of the proposal underpinning the nation's cybercrime law.

Assumptions: In our model, three parties namely i) tech-user ii) attacker and iii) policy-maker are involved. Besides benefit-cost assessment, an attacker learns about the tech user's level of defense, which serves as a sample for the attackers to learn about that of the entire tech-users population. Therefore, if the tech-user is being attacked with a lack of defense, the attacker will be encouraged to continue. On the other hand, if the tech-user is well-defended, the attacker will be discouraged to continue. In reality, the attacker in some cases receives ransom from tech-user or defender. Despite this fact, this study ignores the attacker's welfare including such redistributed wealth as part of social welfare. Thus in this study, the following specific assumptions are made,

- It is assumed that no relevant other factors, except the risk factor of cybercrime consequences, are changing.
- Here a rational tech user's preferences of self-defense depend on the tech user's understanding of the severity of the risk factor.
- These preferences are stable, total efforts and transitive for maximizing the utility of risk-protective choices.

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

4. Theoretical Background Consumer Choice and Utility Maximization

The progression of digital technologies has been changing economic activities in today's world where cybercrime should not be ignored. 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 asks for a ransom to not undermine that value. If these crimes are not properly addressed, they could significantly reduce overall social welfare received from technology-progressions or increase the social cost of human society in the 21st Century Era. Thus studying cybercrimes from an economics perspective is important for two reasons (Becker, 1968). First, understanding the benefits & costs to the person committing the crime can help in decision committing the crime, which leads to an analysis of the optimal approach to limit this crime, given a certain amount of resources. Secondly, understanding the social costs of a crime can help to determine a socially-efficient level of resources that should be deployed against it. Since the 21st Century humankind prefer a democratic environment over dictatorships country-wise (Rahman, 2021a) and since society is a formation of all characteristics of people & its behaviors, the policy-design goal for a society is not always to eliminate a crime. Rather it is for determining how much and which criminal behavior should be tolerated.

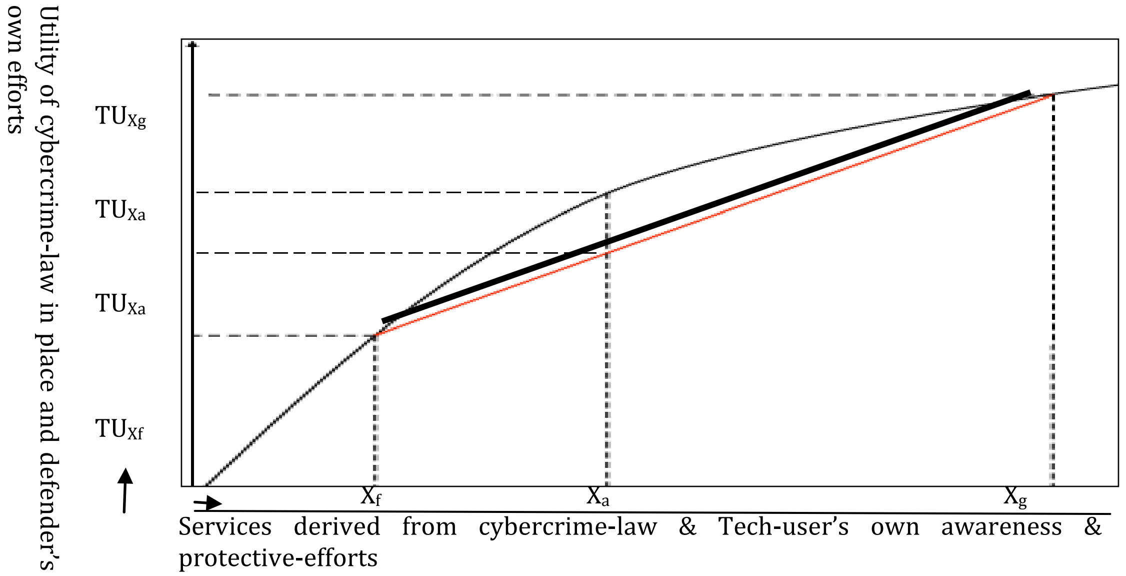
This is because reducing the amount of crime to zero is not necessarily aligned with social interest. This is because a) probable economic cost of eliminating the crime could be higher than its harms to society b) preference based on this cost-benefit assessment can facilitate sharpening and ensuring individual's own responsibility. Thus tech-user has their 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 etc. Since cybercrime is in multi-faceted and complicated issue, in reality, we take freedom and cast a simple example for better understanding why a society decides "how much and which behavior" should be tolerated. Suppose Lavina, a female-gender, wants to see a rape-free human society. To fulfill Lavina's demand, the 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 her. However, it is an essential component for a human growing up for survival no matter what culture or society we live in. It is obvious Lavina's social background, education level, and age, etc. can be instrumental in her awareness & own efforts for her safety besides having the nation's Rape Law in place.

This scenario in cybercrime cases raises the question: how many offenses should be permitted and how many offenders should go unpunished? The method is used to formulate a measure of the social loss from offenses and finds those expenditures of resources and punishments that minimize this loss. The optimal amount of enforcement is shown to depend on, among other things, the cost of catching and convicting offenders, the nature of punishments—for example, whether they are fines or prison terms and the responses of offenders to changes in enforcement. Accordingly, this study proposes a piecemeal approach or separately considering each issue of cybercrime under the general provision of cybercrime where a proposal of a newly established agency or commission can be instrumental for an effective outcome. Under this administration, responsibilities can be broken down based on the type of cybercrime in piecemeal options. The outcome under this setup can be effective where the attacker will be punished and tech-user will be facilitated with training & guidance on awareness and protecting self. Otherwise, the current system may often fail unless they are broken into pieces. In this setup, besides having cybercrime laws in place, the 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.

Awareness & Own-efforts of Tech-users under Theory of Consumer Choices & Behaviors: It is now well recognized that the perceived-risk factor plays an influential role in tech users' decisions (Rahman, 2018; Rahman, 2019). It is no different when it comes to awareness and self-efforts for being on the safe side in case of risk-factor such as cybercrime (Rahman, 2021a; Rahman 2021b). It is palatable to assume that from a rationality perspective, the tech-user is risk-averse, i.e., the tech-user prefers certainty over uncertainty when it comes to saving tech-user from the danger out there. Figure-6 illustrates the risk preferences of a risk-averse for a rational and conscious tech-user who is concerning cybercrime. Tech-user's actual benefit or utility that the tech-user receives from awareness & self-efforts will never fall on TU (X) but rather on the chord (the bold line) as shown in Figure - 6. Point X_g, in Figure - 6 represents probable outcomes of services (X). Here outcome = ƒ (cybercrime laws in place and tech users awareness & own-preventive-effort). That ensures a necessity of joint efforts rather than individual from tech-user or government-cybercrime-law on effectively preventing cybercrime. Accordingly, tech-user may use a certain level of X. Here tech user's awareness & self-effort (AE) = ƒ (age, education level, experience, sense of responsibility, etc.). Thus the outcome of cybercrime prevention depends on strength of cybercrime laws and tech users' awareness & own preventive effort.

It means the outcome of service-on-security depends on full utilization 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 the highest level of security. Any changes to these services-on-security may risk tech-user being a victim. It may cost lower but it can put tech-user at risk. In this setup, X_g represents 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 represents service-on-security derived from cybercrime law where $X_g > X_f$. In the case of X_f, (where X_f indicates cybercrime law in place) tech-user enjoys lower cost, which may produce the outcome of "getting attacked or hacked". As long as 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 represents 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 represents 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 rather EU (X_a).

Figure 6: Cybercrime-Risk Aversion Scenario Having Laws in Place Along with Tech-User's Awareness & Own-Efforts



UAE Government Efforts besides Having Cybercrime-Law in Place: In addition to cybercrime law in place, just recently the government took various steps to strengthen its cyber-security network, particularly within the government entities. The country formed a new council last year to develop a comprehensive cyber-security strategy and help to create a safe and strong cyber infrastructure in the UAE. It is expected that the council will help develop a legal and regulatory framework. So that it can cover all types of cybercrimes and emerging technologies and establish a robust National Cyber National Incident Response Plan to enable a swift and coordinated response to cyber incidents in the country. However, no effort has yet been made that can contribute significantly enhancing the awareness and tech user's own effort for protecting the device. Furthermore, no effort has yet been seen to approach with piecemeal approach addressing the problem, even though it can play a significant role in addressing the cybercrime issues country-wise such as in the UAE. Also, no effort has yet been made by the government on having a self-driven insurance policy such as Voluntary Insurance based on the theme of Akim's Model (Rahman, 2018), which can be instrumental in addressing the problem sooner than delays.

Policy Adoption - Awareness & Own-Effort along with Cybercrime-Law in Place Country-Wise: Welfare Analysis: In an aim to examine benefits of investing tech user's time for awareness & self-efforts besides having cybercrime-law in place for protecting tech-user, this section is designed as follows. It is important for tech-user as well as for the government to get full information about the economic benefits of adopting cybercrime-law and encourage tech users' awareness & own effort for ensuing secure technology usages globally country-wise. Accordingly, welfare analysis is carried-out where findings can be instrumental to policy-makers for policy-adoption decisions. It can also be helpful to tech-user in decisions recognizing the importance of own-awareness and for investing own-efforts on protecting tech-user-self from perceived-risk of cybercrime.

Approaches other than Cybercrime-Law- Policy Guidance Country-Wise such as UAE: Evidence suggests that most governments country-wise have acknowledged the problem of cybercrime by having preventive laws, mostly known as Cybercrime Law. However, the UAE, like many countries has done little engaging tech users for awareness & own effort protecting tech usage. By doing so, people in UAE can be familiar with cybercrime & consequences and can recognize the importance of preventive measures from the tech user's side. It can also provide cyber-security awareness training for employees and develop prevention & response plans.

Guiding Tech-Users on Required Behaviors Facing Perceived-Risk of Cybercrime: In today's world, people are mostly driven by their benefits in multi-faucets such as financial, feeling good, self-recognition, self-pride, self-protection, etc. In this decision-making process, an individual can be a risk-averse or risk-taker. Thus using technology facilitation, the proposed guidance should be in such a way so that both groups can be benefitted aiming to face the perceived risk of cybercrime. Risk-benefit analyses can be useful in delivering the message for convincing tech-users on avoiding risk. Most humans make decisions fairly subconsciously. So, by actually thinking about the risks and benefits of tech users' actions, the tech-user can make better decisions in choices. On the own-efforts aspect, few options the tech-user can choose. They are as follows.

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

Emphasizing Factors that Increase Tech-User's Fondness on Being Safe-Side: In human society globally country-wise, it would not be overstated that using coercive measures such as threats, force, shouting, etc. can have a backfire effect rather than enhancing effective public engagement on a common issue such as the COVID-19 crisis. However, if authorities had devised policies or managed the procedure and explained the importance to follow lockdown laws, have-on-mask, etc. and authorities had provided regular updates about their actions, it would have increased perceptions of the legitimacy of the procedure among casualties

(Rahman, 2018). It would have inspired individuals for investing their own efforts from the beginning for their own safety. Thus, on cybercrime issue, policies are needed now than delaying for inspiring tech-users for own efforts on awareness & protecting self-devise from perceived-risk, the cybercrime.

Welfare Analysis of the Proposal Underpinning Nation's Cybercrime-law: Based on the proposal underpinning cybercrime law in place, the tech user's decision on securing tech-usage environment by setting MPC = MPB in Figure 7. Because of tech users' inspiration, market level of tech user's awareness & own-effort Q_1 and optimal level is Q^* that are generated underpinning nation's cybercrime-law and government's promotional efforts. Area K represents net social gains that are generated by joint efforts of Govt. and the Tech-user's effort. In Figure 8, area (A+B+C+D+E) is tech-user or defender's surplus. The government spending for cybercrime-law implementation is an area (E+B+C+D+F) that 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 the deadweight loss that is just lost.

Figure 7: Welfare from Awareness & Own-Effort Under Cybercrime-Law Implementation

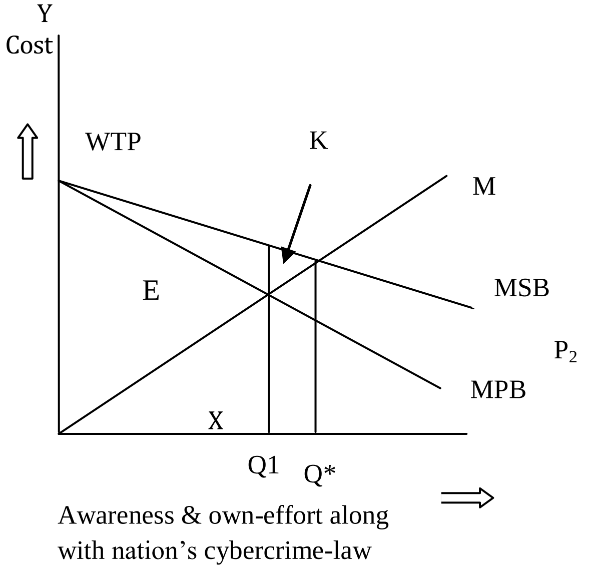
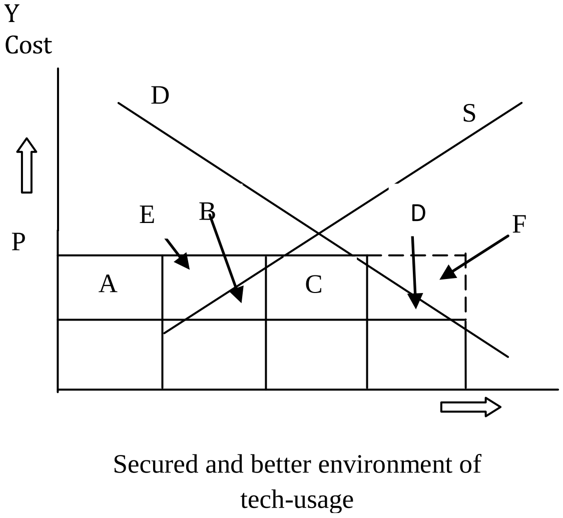


Figure 8: Welfare Aspect of Secured & better Environment of Tech-usage



Future Study: Since cybercrime is a vast and complicated arena, which may get worse parallel to the trends of a growing number of tech-users, it is warranted 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, empirical studies can be conducted for welfare analysis. Further studies can be conducted on the application of Voluntary Insurance in securing digital-banking underpinning Akim's Model (Rahman, 2018). It can further contribute to the understanding, prevention or correction of criminal behavior 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.

5. Conclusion and Recommendations

Conclusion: Today's technology-driven world is counted more in the globe than ever before. The UAE society is no different in the globe. Thus, the decision factors mainly expectancy and cost-effectiveness have led human beings, organizations, agencies or businesses to welcome ICT-facilitations for usages in many folds. As a result, meeting society's needs, many sectors including the financial sector particularly banking services have been modernized. Here customers compete for comparative time-saving option (s) marginalizing its operating costs. With the increase of data usage, the number of tech-users, and devices, cybercrime has been on the rise, which is an all-time high ever since. Only until recent times, we are coming across more and more stories about data breaches and cybercriminal activities. Addressing the issue, like many other countries, the UAE is not out of control by laws.

Since human society is a formation of all characteristics of people & its behaviors, the law for its society is not always to eliminate a crime. This is because reducing the amount of crime to zero is not necessarily aligned with social interest. It can increase probable economic cost eliminating 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 a piecemeal approach in practice where the approach for one department may vary from the approach for another department. Raising tech users' awareness about risky online behaviors and accordingly tech-users are needed 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 lays out the foundations, which can be called 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 costs country-wise such as the UAE with the aim to attract leaderships' attention for addressing cybercrime in a piece-meal 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 a certain portion of utility comes from service-on-security derived from cybercrime law where total utility is greater than utility-received from cybercrime law. Thus the outcome of cybercrime prevention depends on strength of cybercrime laws and tech users' awareness & own preventive effort. It means the outcome of service-on-security depends on full utilization of cybercrime law, tech user's own awareness & self-effort, which can ensure the highest level of security. Thus it costs higher for ensuring the highest level of security. Any changes to these services-on-security may risk being a victim. It may cost lower but it can put the tech-user at risk. From on welfare analysis perspective, the findings show that tech users' actions including awareness & own effort, besides government law can create a net social gain.

Which significantly depends on the tech user's actions as a whole. In this case, the tech user's calculated economic surplus is greater than the government's expenses for the implementation of the cybercrime law, which is collected from the UAE taxpayers. 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. Today people are mostly driven by their own benefits in multi-faucets such as financial, feeling good, self-recognition, self-pride, self-protection, etc. Thus, the guidance of tech-users on required behaviors should be in such a way so that both government & tech-user can benefit aiming to face perceived-risk of cybercrime. Risk-benefit analyses can be useful in delivering messages thru multi-faucets for convincing tech-users on avoiding risk by their own actions. Furthermore, it can facilitate sharpening and ensuring an individual's own responsibility, which can be the by-product of Akim's Model-2021, no matter where tech-users reside in the globe.

Recommendation: Thus underpinning the findings, the recommendations in summary in this study are as follows,

- Provisions under the cybercrime law for ensuring tech user's 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 etc.
- Provisions must ensure a piecemeal approach where a newly established agency or commission can be instrumental for an effective outcome. Under this administration, responsibilities can be broken down based on the type of cybercrime in piecemeal options.
- The legal & regulatory framework related to cybercrime should be in such a way so that it can cover all types of cybercrimes and emerging technologies and establish a robust National Cyber National Incident Response Plan to enable a swift and coordinated response to cyber incidents.
- Provisions must ensure guiding tech-users on required behaviors facing perceived-risk of cybercrime. It must emphasize factors that increase tech users' fondness for being safe-side.

References

Al Neaimi, A., Ranginya, T. & Lutaaya, P. (2015). A framework for the effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, 4(1), 290-301.

Barrett, M. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST Cybersecurity Framework. https://doi.org/10.6028/NIST.CSWP.04162018. Retrieved from https://www.nist.gov/cyberframework

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).

Becker, G. S. (1968). Crime and Punishment: An Economic Approach, Journal of Political Economy, 169-217.

Creesey, R. & Nayfeh, M. (2012). Cyber Capability in the Middle East: Seizing Opportunity While Managing Risk in Digital Age. Booz Allen Hamilton.

Chandra, G. R., Sharma, B. K. & Liaqat, I. A. (2019). UAE's strategy towards the most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 8(12), 2803-2809.

Cherrayil, N. K. (2016). Cybercrime Cost UAE Dh5.14b This Year. Published: 22 November 2016. Retrieved from https://gulfnews.com/technology/cybercrime-cost-uae-dh514b-this-year-1.1933736

Cybersecurity & Infrastructure Security Agency. (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

Dubai Electronic Security Center. (2017). Establishing Dubai as a global leader in innovation, safety and security. Dubai Cyber Security Strategy, Dubai, Government of Dubai. Retrieved from https://www.desc.gov.ae/

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

Economist Intelligence Unit. (2018). Cyber-attacks: is the GCC prepared? Retrieved from https://www.eiu.com/industry/article/806588464/cyber-attacks-is-the-gcc-prepared/2018-04-03

Furnell, S. (2003). Cybercrime: Vandalizing the Information Society. The Lecture Notes in Computer Science book series. International Conference on Web engineering, Retrieved from https://www.researchgate.net/publication/220468582_Cybercrime_Vandalizing_the_Information_Society

Grant Thornton. (2017). Cybercrime: Avoid paying the price – protecting your business. Executive Summary Report. Grant Thornton, United Arab Emirates. Retrieved from https://www.grantthornton.ae/globalassets/1.-member-firms/uae/may-2017-onwards/cybercrime_avoid-paying-the-price_2017.pdf

Gulf News. (2021). How to protect yourself against the threat of cybercrime: UBF's Fraud Awareness Campaign seeks to educate customers on cyber fraud risks. Published: 30 June 2021. 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.

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.

Kshetri, N. (2013). Cybercrime and cyber security in the Middle East and North African economies. In Cybercrime and Cybersecurity in the Global South (pp. 119-134). Palgrave Macmillan, London. https://doi.org/10.1057/9781137021946_6

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

Lewis, J. A., Smith, Z. M. & Lostri, E. (2020). The Hidden Costs of Cybercrime. The Center for Strategic and International Studies (CSIS), Published: 09 December 2020. Retrieved from https://www.csis.org/analysis/hidden-costs-cybercrime

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

Nord, VPN. (2020). 50 countries by vulnerability to cybercrime. Retrieved from https://nordvpn.com/cri/

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. (2019). Microeconomics *Basics*: New Way Learning Microeconomics in the 21st Century Era, Print Your Book Academic Publishing, ISBN 978-0-9557163-0-0

Rahman, A. M. (2021a). CO_2 Emission from Brickfields in Bangladesh: Can Ethical Responsibility by Doin*g* Reduce Level of Emission? *Athens Journal of Social Sciences*, 8, 1-17.

Rahman, A. M. (2021b). COVID-19 Brings Blessing for Digital-Banking in World-Economy Country-Wise: An Analysis under Demand-Supply Model of Market Economics, *Journal of Business and Economic Development*, 6(2), 65-72.

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.

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

Vanderbilt University. (2020). Former FBI Special Agent has advice on hacking risks – Schmidt Lecture November 19. Retrieved from https://engineering.vanderbilt.edu/news/2020/former-fbi-special-agent-cybercrime-expert-has-advice-on-hacking-risks-schmidt-lecture-nov-19/

Walls. (2001). Typology of cybercrime Cybertrespass.

Zaharia, A. (2021). 300+ Terrifying Cybercrime and Cyber-security Statistics (2021 EDITION). Retrieved from https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Acknowledgment: Authors thanks Miss Lavina Moureen Zaman, a College Student, for agreeing & answering all questions she was asked. Her answers are utilized as an example in this article for expanding logical arguments. Thus we say to her "Thank you".