UNIVERSITY OF ASIA PACIFIC

Department of Computer Science and Engineering

Course Title : ICT Law, Policy and Ethics

Course Code : CSE-407

Topi : Role of Software Engineers in Shaping-up the Cyber Security Law in Bangladesh

Submitted by:

Group 2

Section: A

Submitted to:

Alida BInte Saqi

Lecturer

Department of Law and Human Rights

University of Asia Pacific

Name: Afroz Jahan Vabna
ID: 19101011

Role of Software Engineers in Shaping-up the Cyber Security Law in BD.

Introduction: Bangladesh does not have any officially recognized cyber security law against cyber crimes but there are some main substantive laws which are used against cyber crimes. These laws are created to prevent and protect the people of Bangladesh from cyber crimes but these laws have some insufficiency which can be shaped up with the help of Software Engineers. Basically cyber security is the application of technologies, processes which are connected with internet and uses to protect systems, networks, programs, devices and data from different types of cyber attacks. The use of internet and digital devices are now increasing massively and some people misused the applications which leads to various types of cyber crime. To solve this kind of crime that has threaten the security of people, cyber security law had been created under several act. Laws related to cybercrime are Bangladesh the Penal Code, 1860, Bangladesh Telecommunication Act, 2001, Information and Communication Technology Act, 2006 and The Pornography Control Act 2012. All of these laws deal with unauthorized copywriting, introduction of virus, tempuring computer source documentation, use internet and email for illegale activites, pornography and ~~email for illegale activities~~ so on. Moreover, technologies are improving rapidly and hackers groups

are strongely growing up day by day in Bangladesh. who's work are not limited into just hacking. They are constantly creating new threats through dank web that can not be handled with our existing laws. As the technology is constantly updating and the crime patterns of criminals are changing, the rules should be framed keeping these aspects in mind. It is not possible to know all the information of technological updates or predict which types of cybers threats are coming in future for any non-technical person. So, in these cases, Software Engineers can play the most vital role in shaping up the cyber security law.

Cyber Crimes in Bangladesh: Currently, people are exchanging their valuable information using different types of applications over the internet in Bangladesh. compared to any previous time. Most people have no idea how to protect their personal data, which cyber-criminals are using as an advantage against them and as a result, recently the numbers of cybers crimes in Bangladesh has increased

a lot. Software piracy, cyber defamation, hacking, password cracking, credit card fraud, cyber identity theft, credit card fraud, cyber identity misused for defamation, cloning of website, phishing attacks, pornography, virus dissemination, cyber stalking etc are the most common cyber crimes in Bangladesh.

Hacking is the most commonly committed crimes where hackers controls a computer system without the permission of the computer owner/user illegally and they embezzle money through raiding bank accounts, credit card fraud, telephone call selling, product/service fraud.

Besides that, attackers spread different types of viruses to affect the data of important documents. For example; government's offical information, bank's financial documentes etc.

Therefore, cyber bullying or harassment are increased recently in a noticeable amount. According to the records, mostly girls are the victims of cyber bullying or harassment. In some cases, many of them end up commiting suicide due to cyber harassment.

Name: Afroz Jahan Vabna
ID: 1910104

Page:

In addition to the above cybercrimes, there are many other types of cyber-crimes occurring in Bangladesh. Due to the lack of appropiate laws, the numbers of the cyber crimes are continuously increasing.

Name: SHAWAN DAS
ID: 19101020

Page:

Cyber Security Law in Bangladesh:

With the rapid growth of information and technology and use of the internet, Cyber crime has increased in Bangladesh. in recent years. We have several laws to deal with cyber crimes. such as "Information and Communication Technology Act, 2006; Digital Security Act, 2018, Intellectual Property Law(IP), Bangladesh. Though the Digital security Act, 2018 was passed with aim of ensuring Digital Security and identification, prevention, suppression, trial. offences commited through digital devices. Some sections can be used to prevent cyber crime in Bangladesh.

The Digital Security Act. 2018 which was created by modifying Information and Communication Technology Act, 2006 section: 54-67. According to the Act, if any person intentionally do any activity. without the. permission of the owner. such as.

Access or secure access. to such computer, computer system or networks for the purpose of destroying or retrieving. or collect information.

Download, copy, extracts. any data, computer

database or information or data held or stored in any removal storage.

Introduce or causes to introduce any computer virus into any computer networks or computers system.

Damage or causes to be damage willingly or un-willingly in any computer, computer system, computer networks data or database or any computer program.

Denies or causes to denial ob access to any person, Authonized to access and computer system or computer Network.

are punishable abbeeses under section-27, subsection 1, clause-a,b,c ob Digital Security Act, 2018. Whoever commits those obbenses, s/he can be punished under section-27, subsection-2,3, with imprisonment bor a three (3) years to imprisonment bor life, or with bine taka-1crore to 5crore or with both.

Under Section-18, subsection-1, clause-a,b. ob Digital Security Act, 2018 ib any person makes or abets to make illegal access to any computer,

computer system or network to commit an offense, s/he can be punished with fine or imprisonment or both under section-18, subsection-2,3.

Under Section-28 of Digital Security Act, 2018. if any person or group willingly or knowingly publish or broadcast anything on a digital platform that can hurt anyone's sentiment, s/he can be punished with imprisonment for not more than 5 years or fine not exceeding 10 lac or imprisonment not exceeding 10 years or with fine not exceeding 20 lac or with both, Under section-28, subsection-2,3.

Under section-56 of information and Communicati Law, 2006. if any person with the intent to cause or knowingly causes wrongful loss or damage to the public or personal property through illegal access to any such computer, computer networks or other electronic system, s/he can be punished with imprisonment for a term which may extend to taka 1 crore or with both.

If any person willingly or knowingly violate Copyright act, such as piracy of cinematograph film, publish any copyright protected confidential document of an organization, copy/download/share any copyright protected computer program, s/he can be punished under section 82, 83, 84 of Intellectual Property Act of Bangladesh.

According to section-4, subsection-1, 2, 3 of Digital Security Act, 2018, if any person commits any of those mention crime beyond Bangladesh but commited in Bangladesh or commit offense within Bangladesh, from outside of Bangladesh using any computer, computer system or Network situated in Bangladesh or commits offenses beyond Bangladesh, from outside of Bangladesh, s/he can be punished under Digital Security Act, 2018.

Name: Nakiba Nurein Rahman
ID: 19101039

Page:

Cyber Crime Investigation and Trial Trial Procedure in Bangladesh:

To prevent cybercrime and regulate e-commerce, The ICT Act, 2006 was enacted in Bangladesh. The Act No. 39 of the year 2006, came into force on the 8th October 2006 to provide legal recognition to digital signatures, legal framework for E-governance, offences & penalties, adjudication and investigation & trial of cybercrime.

Cyber Crime Investigation in Bangladesh w.r.t. ICT Act, 2006:-

- According to The chapter VIII, Section 76, titled as "Investigation of Crime", any ~~offences under this act offence under~~ offence committed under this act shall be investigated by the Controller or any officer authorized by the Controller, ~~or~~ or by any police officer not below the rank of Sub-Inspector of Police and any offence committed in violation of this Act shall be a non-cognizable offence.
- According to the chapter VIII, Section 80, titled as "Power of seize or arrest in public place, etc."; Any investigation taken under this act, the Controller, or any authorized officer or any police officer not below the rank of a Sub-Inspector of Police, having written the reasons, may enter the public place and search and seize the germane materials and arrest the concerned person or the offender.
- According to the ~~T~~ Chapter VIII, Section 81, titled as "Procedure of search, etc." Subject to the provisions of this Act, the provisions of the Code of Criminal Procedure shall apply to all investigations, entries, searches, and arrests made under this Act.

Name: Nakiba Nurem Rahmam
ID: 19101039
Page:

Cyber Crime Trial Procedure w.r.to ICT Act, 2006 :-

- According to the chapter VIII, Section 68, titled as "Establishment of Cyber Tribunal" The Govt. shall by notification in the official Gazette, establish one or more Cyber Tribunals at times for the purposes of speedy and effective trials of offences committed under this Act. The Cyber Tribunals shall be constituted by a Session Judge or an Additional Session Judge appointed by the Govt. and similarly appointed a Judge as "Judge, Cyber Tribunal".
- According to the chapter VIII, Section 69, titled as "Trial Procedure of Cyber Tribunal;"

1) Without a written report of a police office not below the rank of Sub-Inspector or the prior approval of the Controller or any other officer authorized by the controller, the special tribunal shall not accept any offence trial.

2) The Tribunal shall follow the rules mentioned in the chapter 23 of the Code of Criminal Procedure if they are not inconsistent with the ~~rules~~ rules of this Act, which is used in Session Court.

3) Any Tribunal shall not suspend any prosecution without having written reasons and unless it is required for the sake of just adjudication.

4) If the accused person has been absconded and it is not possible to arrest him and produce him before the Tribunal and there is no possibility to arrest him immediately, in that case, the Tribunal can order the accused person to appear before the Tribunal by publishing such order in two mass

~~a~~ circulated national Bengali ~~dal~~ dailies and if the accused person fails to do so, the prosecution shall take place in his absence.

5) The rules mentioned ~~above~~ shall not be applicable if the accused ~~of committing a punishable~~ person fails to appear before the Tribunal or absconded after getting ~~fail~~ bail.

6) The tribunal can ~~after~~ order any police officer or the Controller, or any officer authorized by the controller, to reinvestigate the case and submit the report within the stipulated time to the Tribunal.

- According to the chapter VIII, section 71, titled as "Rules relating to bail, The Judge of the Cyber Tribunal shall not bail any person accused of committing a punishable crime unless the Govt. side is given a hearing opportunity on similar bail orders or there is reasonable cause in favor of the accused person might not being proven guilty in the trial or the offence is not severe relatively, and the punishment shall not be harsh enough even if guilt is proven.
- According to chapter VIII, section 72, titled as "Time limit to deliver verdict", the Judge of Cyber Tribunal shall give the verdict within ten days from the date of completing of taking evidence or debate, unless he extends the

time limit no more than ten days with having written reasons.

- According to the chapter VIII, section 74, titled as "Prosecution of offence by Session Court", Regardless of what is in the code of Criminal Procedure, the Session Court shall prosecute any offence ~~committ~~ committed under this Act until the special tribunal is established.
- According to the chapter VIII, Section 75, titled as "Prosecution ~~of~~ procedure followed by the Session Court", To prosecute any offence committed under this act and ~~trial~~ tried in Session Court, the session court shall follow the rules outlined in Section 23 of the Code of Criminal Procedure that apply to Session Court trials. Furthermore, regardless of what is contained in the Code of Criminal Procedure, any Session court shall not accept any prosecution/trial of any offence committed under this Act, without a written report from a ~~police~~ police officer not lower than the rank of Sub-Inspector of Police and prior approval of the Controller or any officer authorized by the Controller.

Name: Zarin Tasnim
ID: 19101003

Page:

Comparison between Bangladesh Vs other countries cyber security law:

Regarding Bangladesh, we do not have a cyber security law except the conventional Information & Communication Technology (ICT) Act, 2006 and the Digital Security Act (DSA), 2018. In the wake of ultra-advancements in surveillance techniques over the last 10 years, the existing legal structure is not sufficient to cope with the newly manifested threats. As of today, in Bangladesh, any sort of spyware is illegal because spyware or malware enables cybercrimes under the ICT Act, 2006 and the DSA, 2018. In order to check the misuse of surveillance technologies, the existing cyber law needs to be amended or a dedicated cyber security law should be enacted. Besides that under the Information Technology Act of 2006, the I.T. Act's 2013 update or Bangladeshi law, cybercrime is not specifically defined. Due to the lack of a clear definition of cyber crime, in Bangladesh there many spectacular observations can not be analyzed properly.

Now if we try to overlook the cyber security related laws of other countries, then we will be able to compare them as well as will be able to identify the shortcomings of our country's law. Thus we can get suggestions of ways to improve the lack of our country's cyber security related law and ensure the cyber security than before.

⇒For instance, if we try to overlook the cyber security law of USA → which is known as one of the most secured countries in the world where cyber crimes are being handled more consciously. We can find here "The State and Local Government Cybersecurity Act of 2021" has been designed to improve co-ordination between the Cybersecurity and ~~Infrastructure~~ Infrastructure Security Agency (CISA) and state, local, tribal and territorial governments. Moreover, in USA's cyber security law we can see the below key points which is really appreciable compared to us.

- They intend to develop a ready Cyber Mission Force and associate cyber workforce where they have included efficient software engineers which can be an important initiatives regarding Bangledesh's cyber security law scenario.
- They have also considered developing policies to support the National Initiative for Cybersecurity Education in their law. Besides that they have also considered taking steps for the necessary knowledge, training other nations to help them to gain the resource and skills related cyber safety issues. Here this training sessions can help our country's software engineers to enlighten themselves as well as others to ~~avoid~~ spread awareness about cyber crimes and ~~to~~ proper solutions of this.

⇒ After that if we try to overlook the cyber security law of Japan, we can find that it has a dedicated cybersecurity law called "The Basic Cyber-security Act", which was enacted on 6 November, 2014. Here we can find the below ~~four~~ strategies:

- In order to raise awareness, they have taken initiatives of activities which they have started from the elementary and middle school education stages. This is really a very promising steps for spreading awarness among the general people about cyber ~~secter~~ security. In our country, this can be included in our cyber security related law.
- Besides that, here in their law, we can find that they have also taken actions to protect critical infrastructure in their law, which will help to make people understand about cyber security.

⇒ After that if we try to overlook the cyber security law of Singapore, we can find that it has 'The Cybersecurity Act', which came into force on 31 August, 2018. Here we can find the below analysis:

- They have taken intiatives to develop a vibrant cyber security ecosystem comprising a skilled workforce, technologically-advanced campigns and strong research collaborations so that it can support Singapore's cyber security. ~~This initiatives~~ These

initiatives are not appropriately present in Bangladesh's cyber security related law. So, these scenario can be included.

- Besides that, they have also taken initiatives to introduce scholarship programs and industry oriented curriculums, while-up skilling and re-skilling opportunities for mid-career professionals. This will be provided through initiatives such as the Cyber-Security Associates and Technologists Program.

Moreover, if we overall try to compare Bangladesh's cyber security related law with the above mentioned countries' law, we can get the analysis of the fact that:

- Here we need to increase the capability of cyber security professionals in Mangerial, Technical and information assurance areas which is not sufficient compared to other countries.
- Then we need to add more cyber security awareness to the national education curriculum as a way of spreading knowledge to pupils & their relatives
- Therefore, it may be more helpful to create training sessions like the other countries to train senior policymaker, governmental officials about the threats to electronic networks and how these networks can be effected by cyber crimes.

In conclusion, we can state that compared to other countries, Bangladesh's cyber security related law is kind of not so well organized.

Civil & Corporate feedback on Serious Cyber issues:

As Bangladesh doesn't have any authorized cyber security law against cyber crimes and about 37% of softwares that is used in Bangladesh is pircated in Corporate Companies. Cyber Crime & policy is the most concerned issue here. We have talked with some professionals regarding this issue and got some useful reviews. Their opinion is written below →

"Biggest threat for cyber security in corporate sectors are hackers. in our country or outside of our country. For example, a few days ago Bangladesh Bank incident. Bangladesh Bank faced a problem because of hackers, as it was a small incident we could solve it by ourselves. These security systems needs to be more updated."

He also added that –

"cybero crime Law should be enforced strictly so that no one can ever try to commit these crimes online and software engineers can play an important role by enhancing the security of the softwares people are using.

How wee keep maintaining our house security that's how we need to be strict with the online security. Last but not the least as it is an important and most of the world depends on software and online ~~in~~ nowadays."

Said by - 'Dr. Aloke Kumar Saha,
Professor, Dept. of CSE,
University of Asia Pacific.

From the above interview we can realize the importance of softwares engineers role against cyber crime. They can ensure the security by enhancing or updating the software security.

Another review we are adding below—

According to his point of view " Maintaining the security of data is the main concern as attackers can access the data and use them. Software engineers can play an important role about data processing. Security and can reduce the cyber crime."

From the interview here we can also say that securing the cyber crime law software engineers can play an ~~im~~ important role.

We took some polls for knowing the cyber crime and it's law effect in Bangladesh and how important people thinks about it—

According to the polls, around 91%. of people (age below 18 to 35) thinks that cyber security law is not implemented well and 84% of the people thinks that

software engineers can shape up the cyber security.

As we can see, 84% of people thinks that software engineers can shape up cyber security. So, people think that they are an important role to play in cyber security.

So, software engineers should come foroward and play an important role by updating the security systems of softwares. That's how software engineers can ensure and protect cyber security and cyber security law.

Name: Md. Hasibur Rahman
ID: 19101009

Impact of Cybercrime in Software Industry:

Cybercrime has become a growing concern in Bangladesh. During the last decade Bangladesh has done a revolution with technical enhancement. With unauthorized intervention to the system, many companies lose confidential information which causes financial loss, privacy issue for its users, shareholders. All cybercrime is performed by abuse of electronic media, using computer system, top listed cybercrime is mentioned before,

The reason for cybercrime described by Hart in his work "The Concept of Law" has said "human being are vulnerable so rule of law is required to protect them". The vulnerable cyberspace creates vulnerability and it needs to be protected against cybercrime. So the need for cyber protection law comes. Reason behind may be said to be: Negligence, Complex interface to user, easy to access, loss data capacity. Now we will discuss about major impact of

Name: Md Hasibur Rahman
ID: 19101009

Cybercrime on software Industry:

Unauthorize control over system:

It is commonly reffered as hacking. Some individual or groups of hackes may take control over a system which do not belongs to them. This contral may leak major inmate information of the company. In retaliation of creating of the movie "The Interview", a north Korean hacker group phished through media giant Sony Entertainment on 2014. It cost them $100 million.

Software pirate and Copyright:

A company, software farm build Software to earn money from selling it. Result of an anonymous experiment conduted on more than 9,800 students in San Diego were presented that

Name: Md. Hazibur Rahman
ID: 19101009
Page:

38 pereent of teenagers were involved in software piracy. In the context of Bangladesh most of the computer users are in the habit of using pirated software. It is clear that It made huge loss and developers as they are not getting paid for their created work. Software vendors around the world lose nearly $96 billion annually to piracy.

Possession of unauthorized information:

Hacker may hack and store the informd-ion of the system. At a reent event, Rackstar games lost $1 million dollar as the source code for upcoming GTA-6 got be leaked by a 17 years old boy. On 2016 Bangladesh Bank lost close to US $1 billion form a online Bank heist.

Name: Md. Hasibar Rahman
ID: 1910 1009

Page:

All modern industries are eveloped around software controled system. all are at risk of cybercrime as many vendos use cheap security protocals, some neglect security and lose money, some are new with the industry. without proper experince, they are also getting cyber attack. The gradual dependence and extensive use of computer and information technology by the vendors like bank, insurance company, and organizations increase the tear of commission of cybercrime.

Oure Software Industry must take initiative unless the reference event may occur in Bangladesh with huge impact on social and economic life.

act. In the time of enactment of this act it was said in section 68 that a special tribunal named Cyber Tribunal will be established in every district of Bangladesh. But till now only one tribunal has been established in the capital of the country, Dhaka City.

* The Cyber Tribunal has not yet punished any criminal. Due to this the criminal are committing more crimes thinking that they will not be punished. This is one of the main weaknesses of the implementation of the Bangladesh Information and Communication Technology Act 2006.

* There is a dependency on technology specialists well trained lawyer and judges with appropriate knowledge of technology. So as a result, recognizing and discarding cyber-crimes has been difficult.

Name: Saiyara Mahmud Prachi Page:
ID: 19101044

* Bangladesh has formed the authority of Computer Emergency Response Team (CERT) where cyber-crimes can be traced with appropriate technology and system management by the specialist But it has the permission to be working only for the necessity of internation CERT and not for the necessity of Bangladesh.

* Information security is an important coordinator for business and more cooperation between countries and across industries. So, in order to safeguard information security, cyber-crime regulations are essential. The lack of an appropriate frame work for information security is one of our challenges.

* With the increasing number of social media and boundary less usage of the internet, the implementation of the existing cyber Security laws has become more challenging. The attacks

of spamming, phishing, spoofing, denial-of-service attacks, worms, malware etc have become alarming as the Cyber Security Law does not provide for any protection thereto. Which proves that the existing rules and regulations are quite cloudy in order to control these Cyber-Crimes.

Name: Saiyara Mahmud Prachi
ID: 19101044

8. Boundary / Challenges of Cyber Security Law in Bangladesh

In the present time of Bangladesh, the occurrences of cyber-attacks continue to increase at various commercial and service providing institutes including banking services accross the country; even after taking multiple safety measures. With the increasing numbers of Cyber Crimes, we can say that the existing laws and its implementation have some boundaries. The insufficiency of existing infrastructure and the lack of appropriate knowledge is the reason behind it. Some challenges of Cyber Security Law in Bangladesh are given below-

* The offenses of the Bangladesh Information and Communication Technology Act 2006 are non-perceptible under section 76(2). The victim has to file an allegation to the law enforcing agencies in order to get the remedy. This is a weakness of the said

Name: Tanmoy Mazumder
ID: 19101013

Page:

How Cyber security laws can be improved:

a) Room for improvement:

The most significant collection of laws related to the cyber security aspect is the Digital security act of 2018. This act has some laws that are not optimal.

In chapter III; Preventive measures, it is stated in section 8 that the law and order enforcing force may work with BTRC To remove any data-information from the digital media. This creates a severe problem as it prevents the free flow of knowledge while trying to prevent crime. As long as a piece of information is true, it should be allowed to exist. Knowledge should never be restricted; rather, the proper way is to research about the information and the knowledge it leads to, so that such measures can be taken that this information causes no harm. for instance, if there is any news that may invoke racial hostility, measures should be taken to prevent that hostility, instead of removing the information altogether. Information should never be sacrificed in order to maintain order.

Furthermore, subsection 8 of the same section states that the executives may alter or override the law

using rules, which create a further possibility of information being removed.

Section 16, subsection 4 mentions that the inspection and examination of safety of any critical information infrastructure shall be conducted by a person expert in digital security. However, there is no definition of the term 'expert in digital security'. This may lead to unworthy individuals to be assigned to the position, which would result in sub-par performance and would hinder the proper and swift execution of the law.

Section 34, loosely defines the act of hacking in a way that would cause even the procedure of regaining control of one's own computer system to be a direct violation of the law.

These examples show that there is much room for improvement in the current law.

b) How software engineers can forward their suggestions:

Software engineers, being capable of identifying the problems in the laws can reach out to the proper authority formally through their engineers' organizations and help make amendments.

Name: Noor Mainukh Khan Annob
ID: 17101038

2c. How software engineers can solve problems mentioned in Point 8

Software engineers can raise public awareness about cyber security law. Their efforts can prove to be fruitful in making law makers, general public, law enforcement authorities more knowledgeable about cyber security; hence increasing standards for cyber security in Bangladesh.

If software engineers' efforts to raise public awareness about cyber security law become successful, the public may let their opinion known to the government that they want a cyber tribunal established in every district of Bangladesh. So the establishment of said tribunal may become faster.

Software engineers who are excellent in cyber security can train lawyers and judges to take more informed actions regarding recognition and discarding of cyber crime.

Software engineers can form a professional body by cooperating with government officials and non-government entities to shape up an appropriate framework for information security.

Cyber security and law aware software engineers can make the general public aware about spamming, phishing, spoofing etc and the legal implications of these actions in the content of laws in action in Bangladesh. Thus the general public may demand to the government that the weak, vague points of the law should be corrected; resulting in stronger cyber security law.

Name: Noor Mairukh Khan Arnob
ID: 19101038
Page:

9 d. How software engineers can help to make laws against crimes mentioned in point 2

Software engineers can put forth suitable laws to prevent piracy of the software they develop. Many software engineers are working in social media sites. They know the ins and outs of the social media sites better than anybody. Therefore, they can suggest laws to prevent crimes like identity theft, cyber defamation, hacking etc. Some software engineers working in the banking industry know about the security vulnerabilities in the banking systems. They can use this expertise of theirs to suggest laws against crimes such as electronically embezzling money from bank accounts, credit card fraud, document stealing etc. Many times, when girls face cyber harassment, they do not contact law enforcement authorities out of fear. In some cases, they contact a family member or a friend who is a software engineer to get advice. Hence some software engineers have a good grasp of what kind of cyber harassment occurs against girls and how it affects them. These software engineers can protect girls from cybercrime by proposing fruitful laws.

Name: Noor Mainul Khan Annob
ID: 19101038

Page:

9e. How software engineers can suggest the latest required laws for certain new threats

Although many software engineers did not study cyber security, many of them are involved in life long learning. They enhance their knowledge of networks, websites, digital assets, encryption, malware, mohitoring etc. everyday. By using their domain knowledge of software engineering and cyber security, they can suggest the latest required laws for specific threats. For example, if a software engineer faces some new kind of security attack while professionally practicing software engineering, he/she may figure out a way to mitigate that attack and derive procedures to prevent it. Software engineers can point out the flaws in existing judiciary systems which serve the purpose security attack prevention. New online services are being deployed everyday. The laws are not updated enough to cover all aspects of modern cyber crime. If a new widespread cyber attack occurs, the software engineers with knowledge of cyber security can work with lawmakers to build powerful laws against it quickly.

Name: Ananna Boiddo
ID: 19101001

(f) Role of software engineers for influencing people in creating public opinion in favor or against a law

It is essential to be properly knowledgeable about the existing laws to take necessary precautions and build awareness for any types of crimes or offenses related to it. Therefore, to create public opinion on the issues of cyber security they need to be informed about the laws related to it, i.e., present cyber security laws, current implementation of the cyber security laws in their country and in other develop countries. Being knowledgeable about these facts they will gain the power to think about the problems and generate multiple views to solve the issues. Software engineers can play a role to convey these types of information to general people.

Over the past two decades new technologies, different delivery methods of information and changing expectations of people have brought tectonic shifts to the relationship between people and information. For example, at present people search for news in different social media or online platforms instead of reading newspapers. Software engineers can take the initiative to build online platforms where people can get information about the laws and current affairs. It is necessary to maintain authenticity of the information for creating

appropriate opinions. Moreover, people need a place to convey their opinion. Software engineers can create this environment virtually and make a proper controlling system for ensuring reliability of the platform. Making people up to date about new laws will influence them to accept or deny the decision. Furthermore, if the software engineers follow principles like not building or publishing products that go against the law, then it will create an impact on people about the law. Besides, if they feel the necessity of adding a new law after facing a cyber issue, they can advertise their proposals to gather public opinion.

(g) Train software engineers about data security and privacy

Cybercriminals try to identify vulnerabilities or weaknesses in computer systems and exploit them to execute attacks. They launch these attacks for various reasons, i.e., personal or financial gain, social or political causes, spreading terrorism etc. To prevent these attacks the computers, computer networks or other computing systems should be strong and stable. It is the duty of software engineers to complete these requirements.

In the laws related to cyber security the topics or areas are not properly defined that is required for a software engineer to obstruct the attacks. A software engineer must be knowledgeable enough about the security and privacy of computer systems and networks. They must know the types of cyber attacks, the motives behind them, the vulnerabilities of a system and how to overcome them. They should be capable of building modern tools and programs in order to build secure system. Moreover, they should also be capable of using and managing these tools and programs, ie., configuring databases to enable access control and encryption, and monitoring for malicious all activities. If these ~~require~~me required qualifications are properly added and mentioned in cyber security laws, there will be more eligible engineers and at the same time their products be will be more secure and strong.

(h) How Software Engineers Can Be Employed To Provide clarification About Cyber Security Law

Laws will be substantiated as effective when general people will understand, accept and follow them. There are a large number of cyber security related laws. However, some laws are not properly clarified in the law statements. If the statements are not properly

narrated, it will be difficult for common people to understand them. Again, without appropriate clarification, it will create troublesome situations when identifying a crime and it's punishment. Since the software engineers understand the terms related to cyber security and they are supposed to be knowledgeable about the laws related to it, they can create appropriate detailed documentations of the cyber security laws. If government appoints software engineer to create clarified documentations of the laws, that will be understandable for general people, then the laws will spread quickly and more public opinion will be created.

Name: Abdullah Al- Mahmud
ID: 19101097

Page:

Future of Software Engineers in Cyber Security Laws:

Now days cyber security has risen to the top of corporate agendas, as business continue to grapple with cyber threats associated with the rise in remote work and increase in online commerce driven by the COVID-19 pandamic. According to research, 88% boards now regard cyber security as a business risk rather than simply a technical problem for IT. There's no easy answer to addressing this. Many aspects of our security strategy and technology need to be improved. What's most important at this time is for organizations to recognize and acknowledge the risks from our supply chains and to demand that we all do better.

Many laws and regulations regarding cyber security are currently being passed on a local and national level, but still most frighten things is that only 25% of less of cyber security incidents are reported, which raises question of What trends we can expect to see in the future.

Looking past 2021, there are a few threats and trends that may make up the future of cyber security. In the greater adoption of new technology will be causing an increase in cyber-attacks. These new technologies are expected to find the roadmap for higher security as well cause cyber-criminal will analyze their malware and launch more advanced attacks, which brings us to the next point we could expect more supply chain attacks and even

more nation-state attacks.

Software engineers can be an asset in strengthening your defense against attacks. The pool of skilled software engineers is growing exponentially everyday se empowering them to build software and applications more securely is one way to help to bridge this gap and also train them how to use new technologies by maintainging proper safety. The programming skills can be applied in designing in analyzing software vulnarabilities and identifying malicious software. With programming expertise, they can also create tools for testing the security of applications and systems.

As we update the technology and software engineers, we need to update the law as well. For better law to prevent the cyber criminal software engineers would help because they are the one of them who knows how to misuse any software or do any harmful work in cyber, introduce software engineers code of ethics in cyber security law would inspire people to follow them. Introduce more child privacy law by knowing from software engineers, what is more needed. Introduce law that inspire people to ask any type of help regarding cyber-crime. Introduce law about software engineer helping to catch criminal under cyber-crime.

It's hard to look at the calender and make predictions about what the future will hold, espicially in an industry

Name: Abdullah-Al-Mahmud
ID: 1910147

page:

as complex and fast-paced as cyber security. But at the end we have to aware people, inspire people not only the IT person but the non-IT also about ethics. And also, about protecting themselves how they could be safe and how they could keep others safe.

Conclusion:

Our government has been working towards the betterment of the cyber world, by enacting laws and regulations as well as cyber tribunal as the initial steps. Apart from introducing new laws and provisions the main think is ethics. If software engineer or people does not follow ethics the knowledge won't help them to prevent things. It is important we train our people, police, judges and advocates about the cyber world. It will help us implement cyber laws properly and ensure qualified resources to fight against cyber criminals.

But after all of discussion, it is very important to say that without proper education about the internet and then we can not make safe house of internet. To make a digital country it is very important to

Name: Abdullah - Al - Mahmud
ID: 1910147

page:

make a strong law on the basis of situation. If we follow that recommendation then we can find the solution at all. Cyber security is a must need for us in modern era. It is very important to think that all cybercrimes are like as civil crimes we have to protect our country immediatly. And we must follow and respect the law.