Awareness and Overview of Saudi Cyber Law

Bushra Qayyum, 
Jubail University College, Jubail, Saudi Arabia 

& 

Rawan M. Alharbi, 
Jubail University College, Jubail, Saudi Arabia

& 

Reham Alamri 
Jubail University College, Jubail, Saudi Arabia

Abstract—With rapid growth and utilization of the Internet, cybercrimes are becoming more serious and divers. New laws and roles should be establish and implement with a specific end goal to control cybercrimes. Saudi Arabia actualized anti-cybercrimes laws to protect its people from different sorts of wrongdoings and to enhance the information security. This paper discusses the impact of cybercrime in our daily life and examines the nature and types of crimes considered under Saudi cyber law and penalties applied for law-breaking. Finally, an online survey is conducted to analyze the awareness of Saudi cyber law among the people living in Saudi Arabia. Result shows that people have awareness about cyber law but they are lacking of risks and penalties associated with law-breaking.

Keywords---Cyber crime, Saudi Arabia, penalties, challenges.

I. INTRODUCTION

THE rapid growth in telecommunication, computer hardware and software and the availability of more powerful and cheap devices allows all type of business large or small and individuals to reach and use the Internet more easily and significantly. Organizations started to use the internet in all of their transactions and operations as well. Individuals also use the internet almost every day at work, home, schools and in any other places to access many websites and applications such as social networking sites, emails, play games and etc. This rapid use and growth of information technology required better methods and laws to protect devices and information from disclose and cybercrimes.

Cybercrimes refers to any crime that include the use of internet or computer networks such as web defacement, hacking, fraud, scams, copyright infringement, service denial attacks and any other unethical acts using the internet. The internet users are the victims of cybercrimes from any ages and nationalities. They can be individuals, organizations, and governments. Cybercrime is increasing and expanding day after another since most of individuals and businesses have switched to online transactions. They became a business that uses technology to perform effective and unprecedented crimes. These crimes have huge scale and effect. Protecting individuals and organizations from these cybercrimes became necessity. Therefore, many countries realized this danger and started to implement anti-cybercrimes laws in order to fight this type of crimes such as stealing, accessing or misusing information without a license, phishing, or shutting down or misusing websites or computer networks.

Saudi Arabia one of these countries that took cybercrime seriously and implemented anti-cybercrimes laws to avoid information security breaches and to protect its people from these crimes. Due to the huge economic costs of cybercrimes in Saudi Arabia it recognized the importance of setting laws to fight the globalized cybercrime and punish its perpetrators. The government seeks to develop systems and laws to keep pace with an update in the world of cyber-crimes and the introduction and development of methods of disclosure and follow-up and the discovery of conclusive evidence.

Bushra. Qayyum. is with the Jubail University College, Jubail, and 31961 Saudi Arabia (corresponding author; phone: 033 3453480; e-mail: qayyumb@ucj.edu.sa).

Rawan. M Alharbi, Reham. Alamri are with the Jubail University College, Jubail, and 31961 Saudi Arabia (e-mail: s32120021@ucj.edu.sa, s31120042@ucj.edu.sa).
The Council of Ministers of Saudi Arabia approved the IT Crime Control and the Electronic Transaction laws. These two laws provide serious fines and penalties for any electronic misbehavior such as blackmailing or stealing from bank accounts or financial bond funds. They may also include terrorist acts such as hosting or designing websites for terrorist organizations. The purpose of the two laws is to prevent cybercrimes, identifying crimes and their respective penalties and identifying the component agencies responsible for follow up on such crimes. They result in Achievement of information security, protection of the rights related to the legal use of computers and networks, safeguard the public interest, morals, and ethics and protect the national economy.

II. RELATED RESEARCH WORK

The benefits of the internet are continuously growing with the development in technology. However, these benefits have huge numbers of cons and risks. Cybercrimes are continuously increasing and spreading globally. The internet attackers can be from different countries and they can harm the government, economy, organizations and individual as well as in many ways. Therefore, many countries have been developed anti-cybercrimes laws to protect their people [1].

In recognition of this, the Council of Ministers in the Kingdom of Saudi Arabia approved the IT crime Control and the Electronic Transaction laws to combat cybercrimes in March 2007 [2]. The law aimed at control and govern the growing number of cybercrimes and determine fines and penalties for these crimes [2]. The public interest of the development of these laws is to secure the use of computers and the international information network (the Internet) and to protect people from hackers who commit electronic crimes [2].

The law contained 16 articles that describe the nature of crimes and the fines and penalties applied to these crimes. These articles also specify what governance body responsible for its implementation and provide ways to control, limit and reduce the occurrence of such crimes in the future [2].

The first article identify the terms and phrases of the cyber laws. If these terms and phrases mentioned anywhere in the articles they will have the meaning expressed next to them unless the context require otherwise. Person is described as any natural or corporate person, weather public or private. Also, The Information System is defined as a set of programs and devices designed for managing computers. Moreover, Information Network is described as an interconnection of more than one computer or processing data to get, share and exchange data. Furthermore, any Information, commands, messages, voices, or images that are prepared for use in computers or that can be saved, processed, transmitted, or constructed by computers are described as data. In addition, Computer programs are defined as set of commands performed on data to run applications that support different functions. Any electronic devices with system to process, store, present and exchange the data is defined as computer [2].

On the basis of this law, any intentional access by a person to computers, websites, information systems or networks is considered as unauthorized access. Any action include the use of computers or internet in violation of this law is considered cybercrime. Also, website is defined as any online site that provide information on the internet via specific Uniform Resource Locator (URL). Finally, the illegal viewing or getting of date is described as Reception [2].

The second articles describe the goal of this laws which is to limit the occurrence of cybercrimes. This result in achievement in information security, Protection of rights, public Interest, morals, common values and national economy [2].

The third article of this law state that Saudi Arabia has said it will impose 1-year prison sentences and fine of SR500,000 ($133,000) or to either punishment for Internet hacking and misuse of mobile telephone cameras, such as taking unauthorized pictures. Hacking, threatening or blackmailing a person, eavesdropping on, tapping or obstructing information sent through the internet or a computer without legal justification [2].

The fourth article state that any person who reached bank or credit information related to securities ownership to get information or money or services without legal justification will impose 3- years in jail and/or fined an amount not exceeding SR 2 million [2].
The fifth article impose a period not exceeding 4 years in jail and/or a fine not exceeding SR 3 million for stopping the internet from functioning, hacking into a website to delete, erase, destroy, leak out, change or republish personal information [2].

The sixth article indicate that any person who create materials or data related to pornographic or gambling network, producing anything that may encroach upon the public order, religious values, public morals, or the inviolability of private life or preparing such material, sending, or storing it through the internet or a computer will impose a period not exceeding 5 years and/or fined up to SR 3 million [2].

The seventh article state that any person hacking into a website or an information system directly, establishing a website for terrorist organizations and/or publishing it to aid the leaders of these organizations or any of their members, or promoting their ideas, or financing them, or publishing how to make explosives or other weapons used in terrorist acts will impose for a period not exceeding 10 years and/or fined up to SR million [2].

The eighth article state that if the cybercrime combined with one of the following the imprisonment and the fine may not be less than half the maximum: The crime is performed through organized crime, if the offender holds a public office and the crime perpetrated relates to this office, or if he perpetrates the crime using his power or influence, the alluring and exploitation of minors and similar actions or if the offender has been beforehand been convicted of related crimes within or outside Saudi Arabia [2].

Article nine indicate that Any individuals who support or collaborates with others to perform any of the crimes stated in this Law will impose to a punishment not exceeding the maximum punishment designated for such crimes, if the crime is performed as a result of that support and collaboration, but if the crime is not performed he will impose to punishment not exceeding half the maximum punishment designated [2].

The tenth article state that any attempt by any individuals to perform one of the crimes stated in this law will impose him to a punishment not exceeding half the maximum punishment designated for said crimes [2].

Article 11 indicate that if the offender inform the competent authority about the crime before it happened or before it cause a damage, the competent court has the right to exempt the offender from such punishments. Also, if the offender inform them after the occurrence of the crime, he may be exempt from punishment if the information that he offered to the court leads to arrest of the other offenders [2].

The twelfth article state that the enforcement of the cybercrime law shall neither impair the provision of related laws, specifically those regarding intellectual property privileges, nor related international settlements for which the Saudi Arabian Kingdom is a signatory.

Article 13 indicated that the devices, software, and means used in performing any of the crimes stated in this Law or the proceeds generated therefrom may be confiscated without prejudice to the rights of bona fide persons. Moreover, the website or the place where the crime is committed with the owner's knowledge [2].

The fourteenth article state that the assistance and technical support from the Communications and Information Technology Commission must be provided to competent security agencies during the Investigation stages of such crimes and during trial [2].

Article 15 indicate that Bureau of Investigation and office of the Public Prosecutor is responsible for the investigation and persecution of crimes stated in this law [2].

The last article of this law which is 16 stated that the cyber law must be published in the official gazette and will take effect 120 days after publication date [2].

Any person who instigate, assists or plans with others to commit any electronic crimes will be affected by this law and subjected to penalty [2].

However, this law is continuously changing with development and change in information technology. This law is updated to include "naming and shaming" penalty. The law could allow offenders to be publicly named and shamed. This change in Saudi cyber law is an example of using social shaming and naming as a tool to deter criminals from committing these crimes. The courts have
additional power that allow them to publish a summary of the ruling in one or more local newspapers or any other medium in the context of the type of the crime, its severity and its impact. The offender may also pay for the costs of publication [3].

Nowadays, with increasing number of social networking sites such as Twitter and Facebook, Saudi Arabia attempting to include rules and penalties against these sites that allows accounts which promote adultery, homosexuality and atheism [4].

Here is a comparison between cybercrime law in the United State and Saudi Arabia. There are many similarities between the cybercrime laws of United State and Saudi Arabia. First of all, both laws to reducing the cybercrime by punishing the criminals. Also, both laws have an anti-cybercrime law that indicate the most spread crime in each country. Finally, in both laws the penalties are jail and/or fine [1].

One of the main differences between the two laws is that Saudi Arabia use the Islamic law (sharia) is the legal system used for the civil and criminal cases. There are four fundamental sources of sharia law in Saudi Arabia. First of all and the foremost use, the holy Qur’an. Second, the "Sunnah" which is the Prophet Mohammad's sayings and practices done throughout his life. Third is the "Ijma" which is the consensus or agreement of the Muslims scholar. Lastly, the "Qias" or analogy. The last two are used only if holy Qur’an and Sunnah are unclear about a certain issue [1].

Another deference is that although both laws have the same type of punishment, but in Saudi Arabia the punishment depends on the type of crime while in the United State it depends whether the crime was done for the first time or was repeated [1].

Here is some examples of differences in penalty in regards to the amount of fine and the periods of imprisonment. First of all, Computer espionage and abuse crime's penalty in USA often not more than 10 years in jail, but for repeated crime it may reach to 20 years, and/or a fine under Title 18, 18 USC 1030 (c) (1) while in Saudi Arabia, Prison for not more than 10 years and a fine of up to five million riyals. Second, Obtaining information by unauthorized computer access crime's penalty in USA One year to five years in prison and up to ten years if the crime large and/or fine under Title 18, 18 USC 1030 (c) were as in the KSA , Prison of not more than a year and/or a fine of up to 100,000 riyals [1].

One of the worst case example of the cybercrime happened in the USA in October 2014 is that the FBI and other U.S. intelligence agencies believed that Russian government hired attacker to make a serious cyber-intrusion to the U.S. government, but this attack is under investigation [1].

In the other hand, Saudi Arabia government's websites was a target of cybercrime from an outside country attacks. The attackers disable these websites for quite some time [1].

III. METHODOLOGY

The researcher used both Primary and Secondary data. A survey was conducted to know the percentage of people who have awareness about Saudi cyber law and if they agree or disagree with this law. The survey has 6 questions and has been targeted female university students. (58) Of the students responded.

IV. ANALYSIS

Based on the data collected through questionnaire the following analysis is made. For the question “Do you have prior knowledge of what is cybercrime?” the 69.1% of respondents reply was yes. This sums up to 38 respondent’s response

For the question “What do you think are the most cybercrimes deployed in Saudi Arabia?” the 41.1% of respondents chose “Cultural crimes”? This sums up to 23 respondent’s response

For the question “Have you ever faced one of these cybercrimes?” the 83.9% of respondents reply was yes. This sums up to 47 respondent’s response

For the question “Do you know the regulations and penalties that apply to this cybercrimes?” the 66.4% of respondents reply was NO. This sums up to 31 respondent’s response

For the question “Which of the following computer user groups are most vulnerable to Cybercrimes” the 45.5% of respondents chose “Personal users”. This sums up to 25 respondent’s response

For the question “Do you agree with Saudi cyber laws and do you feel it reduces the occurrence of the cybercrimes?” the 61% of respondents reply was yes. This sums up to 34 respondent’s response
From this survey we conclude that although most of the respondents have knowledge and awareness of what cybercrimes are, they lack the knowledge of what is considered and what is not under cybercrimes and the penalties of these crimes, so they might be in risk. Therefore, the government should increase awareness among people about this law. Moreover, most people didn't face this type of crimes which means they know how to protect themselves against these crimes. Also, personal users of the internet are the most targeted group to the cybercrimes since in each house there are one or more users who use the information technology to access internet via computer or smartphone. Therefore, individuals should know how to protect their systems and devices from those crimes. Finally, to fight fast-spreading cybercrime, businesses and governments must collaborate globally to develop an effective model that can control the threat of cybercrimes.

Fig. 1 Awareness of cybercrimes

Fig. 2 Cybercrimes deployed in Saudi Arabia

Fig. 3 Encounter of Cybercrimes
V. CONCLUSION

We started our introduction by listing the importance of technology and how that improves our life. However, everything has advantages and disadvantages, and that exactly what Cybercrimes do which refers to any crime that include the use of internet or computer network. Saudi Cyber Law provide us with knowledge about the different types of cybercrimes and also give an idea on how to protect our network from these crimes.

Computer crime is an overwhelming problem worldwide. It has brought an array of new crime activities and actors and, consequently, a series of new challenges in the fight against this new threat. Policing computer crime is a knowledge-intensive challenge because of the innovative aspect of many kinds of computer crime. We summarized 16 articles that describe the nature of crimes and the fines and penalties applied to these crimes which include identifying the terms and phrases of the cyber laws, the goal of this laws, what Saudi Arabia imposes, and provide competent security in some situation.

Finally, to fight fast-spreading crime, governments should collaborate globally to develop an efficient model which will management the threat. Why? As a result of web users and governments...
face exaggerated risks of changing into the targets of cyber-attacks. As cyber criminals still develop and advance their techniques, they're conjointly shifting their targets — focusing less on felony of monetary data and a lot of on business undercover work and accessing government data.

REFERENCES


[4] Saudi Gazette, Riyadh Monday, 2 June 2014; Saudi Arabia amending laws to monitor social media;