Cybersecurity in Qatar

Tooba Aziz, Asra Marzughi and Hissa Al-Muhannadi
Department of Computer and Science Engineering
Qatar University
Doha, Qatar

Abstract—The Internet is one of the most well-known and important invention of the 21 century that affected our lives and changed the way we used to do things. However, it comes with some drawbacks that needs to be considered and addressed because nowadays cybercrimes, cyberattacks and cyberbullying and many harmful acts has increased the risk of using the IT devices and resources, that is why Qatar is trying to improve the cybersecurity field. By creating a ministry of information and communication technology that focuses on protecting the private information and guarantee the safety of the internet. Moreover, this short research article will discuss and review several studies of cybersecurity in Qatar. And evaluate the issues related to cybersecurity in Qatar as well as the procedures and solutions. As cybersecurity is one of the most important IT field these days.

I. Introduction (*Cybersecurity*)

Cybersecurity is a method of protecting electronic networks and the data to prevent any unauthorized person from accessing them to ensure that no data or information falls into the hands of an unknown person whose intention is unknown. Moreover, recently a dramatic increase in the number of cyber-attacks in all parts of the world has been witnessed, especially after the Covid-19 pandemic since almost all the internet users went online to continue working. With these attacks, the rate of economic losses has increased dramatically. Therefore, cybersecurity has been a top concern in the United States, Russia, and Europe, but it gained popularity in the Middle East and Africa only a few years ago as the peoples of the region began to observe the importance of such a topic. In previous years, the Middle East region tried to catch up with digitization, expansion, and development in information and communication technologies, especially after increasing the use of the Internet in the region. It has become necessary to obtain cybersecurity precaution measures to protect critical network infrastructure. With the increase of Internet users, the rate of crimes and electronic attacks increases, as these actions can lead to economic losses and the dissemination of secret intelligence information, which is an integral part of the national security of any nation. Every user agree that cybersecurity is the main important thing in the internet development. However, it has some drawbacks and issues that while considering them it will be easy to solve.

II. cybersecurity in Qatar

A. Cybersecurity development in Qatar

On June 5, 2017, the Kingdom of Saudi Arabia, Kingdom of Bahrain, the UAE, and Egypt announced the blockade on Qatar and the complete closure of all borders linking the blockading countries to Qatar, whether land, air, and sea. This is in addition to prohibiting dealing in Qatari riyals or even dealing with any bank related to Qatar. The UAE hacked the Qatar News Agency (QNA) website in minutes due to the weak protection of the website. After the penetration, many fake and incorrect news attributed to the Emir of Qatar was published, and a blockade was imposed based on this false news. Cyber-attacks targeted social media platforms and state-owned media platforms to spread false news to intimidate the Qatari people and damage their economy. In addition, this attack caused a successive disturbance in trade and transportation in the State of Qatar and associated financial institutions of the government, society, and economy. Such a heinous incident gave us a vivid example of the importance of owning and developing cybersecurity and protecting networks in the country to prevent a recurrence of such an incident. The State of Qatar has strived to develop its cybersecurity in several ways.

The first step is Qatar's National Information Assurance Framework 103 (NIAF), which is the officially recognized national framework responsible for implementing globally authorized cybersecurity standards. The NIAF provides a guide for all policies, standards, and guidelines. Also, the NIAF provides legislation for cybercrime. In addition, Qatar has implemented a national cybersecurity strategy with the development of an action plan. One of the most prominent points of this strategy is the establishment of a team called the Emergency Response Team (Q-CERT), which is a governmental organization that evaluates efforts to improve cybersecurity in the State of Qatar. As Rafael Dean Brown (2018) also mentioned that Qatar is striving to develop its cyber security by adopting many strategies and plans and striving to work according to globally recognized standards (p.15).

III. Literature review

This literature produces and discusses many aspects of cybersecurity especially in Qatar, and listed pros and cons as well as many issues related to cybersecurity. Several studies related to cybersecurity in Qatar have main focus on the QNA cyberattack such as the research by (Rafael Brown, 2018). As cybersecurity field is increasing rapidly many countries are trying to develop and improve their capability in it as the research on (2021) by Hanan Mohammed, the research evaluated the capability of each country in GCC as well as some other countries in the usage of IT and cybersecurity improvement. The study by Von Finckenstein discussed the issues of cybersecurity in the middle east and north Africa including Qatar (2019). Furthermore, the publication by Fatma

Fadlelmula introduced the same topic. Khalifa Al-Dosari journal that was published by (2020) has discussed a very unique topic related to cybersecurity in Qatar, the topic is about cyber threats before and after FIFA world cup 2022. No doubt that the cyber risk will increase during this period of time, as many people from many countries will come to Doha and there are many possibilities that the visitors belong to parties that aim to piracy. This research article collected all topics from these researches and books and produced it in a simplified and informative way. Such as, pros and cons, issues related to cybersecurity, associated fields, comparison and solutions.

IV. Advantages and disadvantages of cybersecurity in Qatar

The world has developed greatly at this time, as relying on technology and the Internet has become an essential and an important part of our daily lives. Several studies have shown that the countries of the Gulf Cooperation Council, especially the State of Qatar, are interested in the field of cybersecurity and its rapid and remarkable development.

A. Advantages of cybersecurity

Cyber security has several advantages, which are helping to deter digital attacks which leads to the privacy and protection of information. In addition, countries that have effective cybersecurity and are always working to develop it, such as Qatar, are among the first countries to advance digitally and economically. Because, all areas have been dependent on technology and technology must be protected with cybersecurity. Also developing the capability maturity model CMM improved software capability and that was a cause to cyber improvement (Brown, 2019). Furthermore, cybersecurity helps recover leaked data, and it protects networks from unauthorized income, which improves the level of information protection. From a personal perspective, it prevents spyware and protects personal information. As for the financial or administrative perspective, many banks in Qatar, finance companies and various types of companies have developed or are working to develop their cybersecurity because of the many positives found in it, such as that banks, for example, can keep customer data and his cards and any bank information with complete confidentiality and high privacy.

B. Disadvantages of cybersecurity

No doubt that cybersecurity is essential nowadays especially after the pandemic. However, cybersecurity has some drawbacks as there is no system that is fully secure and impenetrable. According to (Finckenstein, 2018) Every facet of daily life, particularly essential infrastructure, is becoming increasingly dependent on interconnectivity. Cybercrime, cyberattacks, and espionage are becoming increasingly common as a result of the route to digitalization, the growth in users, and new technologies such as the Internet of Things (IoT). These types of assault can cause significant economic damage and jeopardize vital intelligence for a country's security. Hackers nowadays have variety of techniques to hack and to do unethical behaviours. Consequently, cybercrime and cyberattacks are the main disadvantages of cybersecurity as mentioned above there is no system that is secure 100%. All countries remember the cyberattack that happened to Qatar in 23/5/2017, Qatar News Agency was attacked and confidential information was released and shared to the entire world. The real case was that this information that was leaked is fake and distorted. However, after this attack Qatar realized that her cybersecurity is not as it should be, even if cybersecurity is improved Qatar must consider and put a percentage of cybercrime. That admits that the main negative side is that crimes and attacks are still available. That will lead to destabilizing internal security and threatening the electronic infrastructure. Moreover, programming errors and bugs may be considered as a drawback of cybersecurity. For instance, the attack that happened to QNA was due to some loopholes and errors, as mentioned this might cause a major threat to the country.

V. Issues related to cybersecurity in Qatar

A. Cyberbullying

Recently, there has been an increase in the letters and comments posted on the Internet that carry hate "hate speech" towards any person or group of people. This phenomenon is called cyberbullying and has recently been classified as a problem that all countries of the world suffer from because it affects the victim's safety and may cause personal psychological crises that could to led further danger, suicide. Therefore, most countries of the world have sought to enact and legislate laws that deter any bully and protect victims' rights. As for the State of Qatar, before 2014, the state only criminalized cyberbullying, but there was no complete chapter detailing all cybercrimes and their penalties. Qatari law did not shed light on cyberbullying in extensive details as it should be, but Article No. 326 in Qatari law states that anyone who harms any person or degrades the dignity of any individual will lead the offender to be subjected to a punishment, which is a fine of QR 20,000 or could lead to imprisonment for a period of up to two years. This law is not detailed for cyberbullying, but it includes several crimes, such as threatening text messages or electronic publications offensive to a specific party. As Muthanna Samara and others (2016) mentioned, Qatar did not previously have a law specifying strict penalties for cyberbullies (p.4). However, this thing faded after the development of technology and the increase in awareness among members of society, and the critical role that the media plays in shaping our thoughts about such crucial issues.

In 2014, a law was issued concerning cybercrime. However, this law also does not explicitly include cyberbullying in the desired manner but still preserves the right of victims somehow. Also, it is entirely different from the old Penal Code that was in force as the new one is much better than the old one. For example, a person who uses any technological means to spread hate speech against any individual or compromise his safety is punished by the law. Muthanna Samara and others mentioned (2016) that promulgating a law to prevent cybercrime is significant progress, but unfortunately, it is insufficient. It should be noted that this law is not enough to stop cyberbullying globally, but more states, over time like Qatar, are enhancing their cyber laws to meet the challenges of our century.

B. *Cybercimes and cyberattacks*

The vulnerabilities of the internet have given countless chances to individuals or groups of people to gain unauthorized access to steal data or generate profits, who are known as cybercriminals. Cyberspace (a world of information through the internet) has several emerging threats. They are cyberattacking, cybercrime, cyberterrorism, and cyberwar. They are explained below:

- Cyberattacks are types of attacks that are launched through cyberspace, criminally or politically, to either destroy, disrupt, disable, or gain control over any infrastructure.
- Cybercrime is an act of using computers or the internet to carry out criminal activities. This could include identity fraud, ransomware attacks and theft of card payment or corporate data.
- Cyberterrorism is a type of terrorism that is not limited to an area, it can target any network or border. It is a politically motivated use of computers to cause severe fear and disruption in society. The motive behind cyberterrorism remains hidden. The impact of cyber terrorism does not only stay in the virtual world but can directly affect people and cause huge losses to organizations.
- Cyberwar is the use of technology in such a way that disrupts the activities of organizations. The motive behind a cyberwar is greed to gain power and control.

Qatar is emerging to be a promising country in many of its sectors, thus causing a lot of attraction for cyberattacks to happen. Many cyber incidents have taken place in Qatar. For example, in August 2012, the LNG gas supplier RasGas in Qatar was infected with a virus in its computer systems, which resulted in all of its data being deleted. Another severe example of cybercrime in Qatar would be what happened in 2017, a cyber-attack was launched through a Qatari news channel known as Qatar News Agency (QNA) which was hacked and displayed inappropriate information. In turn, this led to a blockade and termination of political ties between Qatar and GCC countries. This type of cyber-attack became a cyberwar that affected the people and citizens of Qatar immensely.

Qatar has taken many initiatives to tackle an issue like cybercrime. In 2017, Qatar was shown to be combat cybercrime by ranking third in the Global Cybersecurity Index (GCI). Qatar has many non-profit organizations working towards enhancing cybersecurity within the country like Qatar Foundation and Q-CERT. Qatar Computer Emergency Response Team (Q-CERT) is a leading non-profit organization that is informed of all cybersecurity activities in Qatar and makes sure that cybercriminals are punished properly. Moreover, it maintains a Threat Monitoring System (TMS), which collects security-related data automatically and analyzes any threatening situations. Together with ICT QATAR, Q-CERT has also collaborated with Qatar citizens, schools, and government to manage future threats. It also organizes cybersecurity exercises to deal with cyberattacks to enhance surveillance and monitoring (Tabassum et al., 2018).

Qatar has also been closely working with international organizations. INTERPOL has partnered with Qatar to boost law enforcement for investigating and prosecuting cybercriminals. FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST) is an organization that shares information about threats and collaborates worldwide with security teams, the Cyber Security Division in Qatar is one of them.

As being the host of the FIFA World Cup 2022, Qatar has a huge responsibility to maintain and amplify cybersecurity within the country. One way it could do that is to first raise awareness about cybersecurity and introduce cybersecurity degrees in its universities.

VI. CYBERSECURITY AND HEALTH FIELD IN QATAR

In the recent decade, technology has rapidly changed day by day and continues to do so. One of the industries which are becoming more and more dependent on technology is the healthcare industry. As a result, the healthcare sector has been exposed to many vulnerabilities, making it difficult to perform daily tasks. Most healthcare systems tend to have weak and outdated IT infrastructure, making them vulnerable to the cybersecurity challenges like targeting privacy, financial threats, and medical device security.

The type of cybersecurity threats that are common in the healthcare industry and have been on a rise are:

1) Data Breaches: A data breach is a security violation where the cyber attacker or criminal gains illegal access to the sensitive information of a person, In this case, a patient's contact information, medical tests or prescriptions. This type of information could be sold on the darknet.

2) Phishing attacks: This type of attack is usually through an email, where a user is tricked into revealing their personal information like bank details or passwords. Healthcare organizations could be charged with a lawsuit for exposing a patient's data even though it would not be their fault.

3) Distributed denial-of-service (DDoS) attacks: It floods an organization’s network with a huge amount of internet traffic which makes it impossible to use the network. It could cause communication difficulties between doctors, patients, and medical staff.

4)Ransomware: Ransomware is a type of malware where the cybercriminal infects files, databases, and systems until an amount of money is paid to him.

Some other challenges are healthcare system face are inadequate security controls on medical devices (such as X-Ray machines, ventilators, and vital-sign monitors) and insufficient knowledge regarding cybersecurity among the medical staff.

As the healthcare industry is one of the critical sectors in Qatar, it is taking great measures to bridge the gap between healthcare and cybersecurity. According to the Journal of Emergency Medicine Trauma & Acute Care (2021) Qatari Governmental health care sectors like Hamad Medical Corporation and Sidra Medical and Research Center are among

the active members of the Leading Health Systems Network (LHSN) which is a network that connects organizations with health care leaders to improve healthcare delivery. LHSN lead a cybersecurity project with the growing issues of cybercrimes in healthcare. This project was aimed to identify the current state of cybersecurity in healthcare and the framework of cybersecurity.

During the Covid-19, many healthcare facilities were moved online, which created a lot of anxiety and confusion among the medical sectors. Qatar Computer Research Institute (QCRI), a unit of Hamad Bin Khalifa University in Qatar, was quick to inform and warn about the increase of malicious attackers during the pandemic, as the journal of "Cybersecurity for next generation healthcare in Qatar" (2021) stated. QCRI has also been active in introducing many solutions to combat cyber threats in the health sectors within Qatar. They have created many tools/solutions such as:

1) Guilt-by-association tool which identifies suspicious attacks by analyzing domain addresses' previous movements.

2) A tool that identifies spam emails from their communication patterns.

3) Another tool that which based on hosting infrastructure recommends removing the attack sources.

Qatar is proving itself in introducing cybersecurity solutions for the healthcare industry.

VII. CYBERSECURITY IN FINANTIAL SECTOR

The financial institution is also one of the critical sectors in Qatar. Payment systems are the backbone of any financial system. Thus, the payments systems must be equipped with strong security and encryption methods to the financial stability and maintain monetary policy transmission channels. Furthermore, with the rise of online banking systems, cybercriminals have adopted new ways of stealing money and depositing money into their bank accounts. Some of the most common tools that cybercriminals use to gain access to sensitive information in the banking systems are hacking, remote access trojans and online phishing.

Like any other country, Qatar's banking sector is also a strong target for cyberattacks. To illustrate, in April 2016, Qatar National Bank (QNB) suffered from a huge data breach, the data contained confidential financial information about QNB's customers and credentials of some royal family members. This information was then displayed on a whistleblower website (Tabassum et al., 2019).

The regulator of banking in Qatar, Qatar Central Bank (QCB) has taken steps to increase data security and made sure that all banks in Qatar implement the best practices to protect all financial and personal data against cybercriminals.

VIII. COMPARISION BETWEEN CYBERSECURITY IN QATAR AND OTHER COUNTRIES

After the QNA has been attacked and confidential information was leaked, Qatar worked hard to improve cybersecurity. As Qatar has noticed that her systems are not very secured and there is some errors and loopholes. As a result, Qatar launched a new computer science major which is with cybersecurity concentration at Qatar University. Shires (2019 as sited in Mohamed Ali, 2021) reported that Qatar ranked third after KSA and Oman with a slightly different in their readiness to recover from a cybercrime or a cyberattack and their improvement of cybersecurity. Furthermore, Qatar is really putting a lot of effort to be capable to handle any cyber issue.

TABLE I. LEVEL OF CYBER CAPABILITY

Country	**Measurement** [a]		
	ICT development	***Cyber score***	***Silo***
KSA	HIGH	0.881	A
Oman	HIGH	0.868	A
Qatar	LOW	0.860	A
UAE	LOW	0.807	A
Kuwait	LOW	0.600	B
Bahrain	HIGH	0.585	B

[a.] Source: *INTERNATIONAL COMMUNICATIONS UNION GLOBAL CYBERSECURITY INDEX (2018, as cited in Ali, 2021)*

As shown in Table I. Qatar ranked in top three cyber capability with GCC countries. However, Qatar still needs to work on improving ICT. Also, Qatar strategy and techniques is "norms and values in cybersecurity is showing tolerance, respect and maintain the rights and values of individuals" (Hakmeh, 2017, p. 40).

IX. PROCEDURES AND METHODS

The study adopted quantitative method as data analysis where data was collected from 80 respondents. The research attempts to gain information regarding the following questions:

- Are people in Qatar aware of cybersecurity and related crimes?
- Has COVID-19 caused an increase in cybersecurity issues?

The study uses an online survey as a means of data collection instead of primary data collection (like interviews) due to the precautions and limitations because of COVID-19 pandemic. The target for data collection was 100 participants and they were reached through social media apps like WhatsApp and Instagram. Out of the 100-target population, 80 responded to the questionnaire who were colleagues and friends. The online survey was done through google forms. The survey consists of three demographic questions regarding the gender (male or female), the age of participant (under age 15, between 15 and 19, between 20 and 25, age 25 or above) and level of education (high school, undergraduate, graduate, other). In addition, nine questionnaire items were asked which use five-point Liker scale (ranging from strongly agree to strongly disagree) to get responses from the participants. To present the findings, chart (showing the responses) and graphs are used and to explain those results different statistics are used such as percentages and frequencies.

X. ANALYSIS

This part of the research presents the results and analysis of the data collected from individuals. The results are compared and discussed below.

For the demographic's questions, participants were asked gender, age, and education. There was a total of 80 respondents as mentioned before. For the gender (figure 1), there were 50 participants who were female (63%), and 30 participants were male (37%). For the age (figure 2), there were 3.75% under age 15, 15 to 19 were 18.75%, 20 to 25 were 50% and lastly above age 25 were 27.5%. Regarding the education level (figure 3), there were 2.5% of high school students, undergraduates were 68.75%, graduates were 21.25% and lastly other were 7.5%.

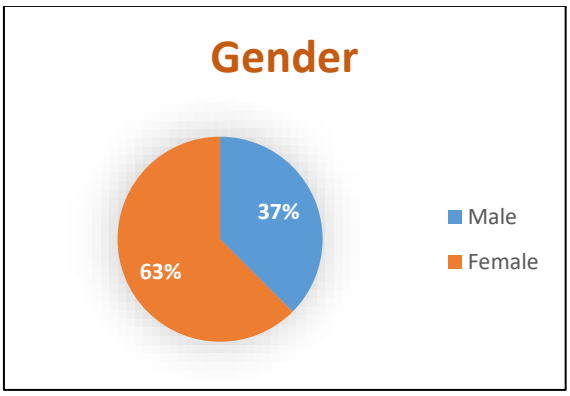

Figure 1. gender of participants

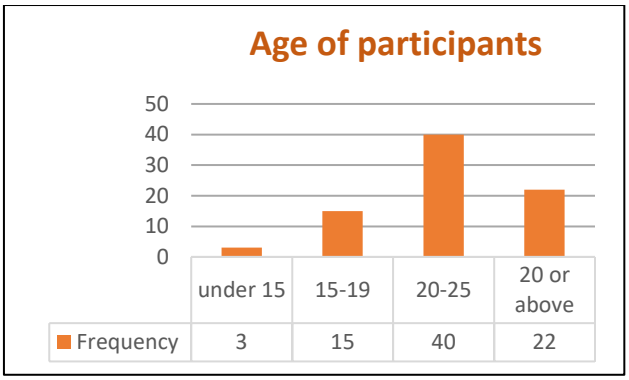

Figure 2. age of participants

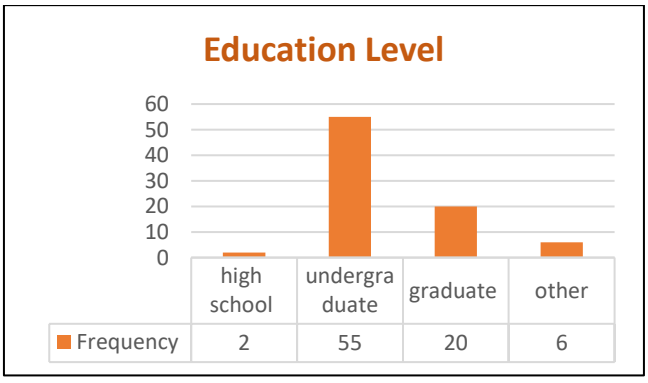

Figure 3. education level of participants

For the nine questionnaire items that were asked these are the results (figure 4). (N=any number) indicates the frequency of people in the survey.

The first question was (I know what a cybercrime is), 75% of participants stated their agreement (N=45) and strongly agreement (N=15). While 11% indicated their disagreement (N=11) and strong disagreement (N=7) was 8.75%. The number of neutral (N=2) participant were 2.5%. These results showed that most people were aware of what cybercrime is.

The second question was (I know of cyber police and cyberlaws in Qatar), where 31.35% were neutral participants (N=25). Majority showed their disagreement (N=30) and strong disagreement (N=5) with a total of 43.75%. A total of 25% of participants stated their agreement (N=15) and strongly agreement (N=5). This indicated that most people aren't aware of cyber policies and laws in Qatar.

The third question was (I use the same password for all my accounts), where majority showed their disagreement (N=30) and strong disagreement (N=20) with a total of 62.5%. A total of 31.25% of participants stated their agreement (N=20) and strongly agreement (N=5). While the minority 6.25% voted neutral (N=5). Results indicate many people know that using strong and different passwords is crucial for security purposes.

The fourth question was (I know where to report to if I encounter any cybercrime). where 25% were neutral participants (N=20). Majority showed their disagreement (N=15) and strong disagreement (N=20) with a total of 43.75%. A total of 31.25% of participants stated their agreement (N=20) and strongly agreement (N=5). This goes to show that a high number of people don't know what actions to take if they come across cyber-abuse.

The fifth question was (I have refrained from providing my information online). 75% of participants stated their agreement (N=45) and strongly agreement (N=15). While 15% indicated their disagreement (N=12) and strong disagreement (N=2) was 2.5%. The number of neutral (N=6) participants were 7.5%. This suggests people are aware of the consequences of giving their information online.

The sixth question was (Cybercrimes can lead to depression), the number of neutral (N=6) participants were 7.5%. 17.5% of participants stated their disagreement (N=11) and strongly disagreement (N=3). The majority of participants showed their agreement (N=35) and strong agreement (N=25) with a total of 75%. The results indicated, many agreed that cyber-crimes could have adverse effect on people's mental health.

The seventh question was (Cybercrimes have risen worldwide during coronavirus), where majority of participants showed their agreement (N=30) and strong agreement (N=10) with a total of 50%. Neutral (N=20) participants were 25%. Participants with 18.75% indicated their disagreement (N=15) and strong disagreement (N=5) was 6.25%. This implies people have come across news which shows the increase in cybersecurity issues around the world.

The eight question was (My data was attacked/stolen during coronavirus). where majority of participants showed their disagreement (N=40) and strong agreement (N=20) with a total of 75%. The minority 6.25% is neutral. While 18.75% of people showed their agreement (N=10) and strong agreement (N=5). This again implies that some people who showed their agreement on the survey, have faced cybersecurity issues due to coronavirus as most of the work and school related activities have shifted online.

And the final question was (Data is not secure on sites (like Zoom, Teams, Google Classroom, etc.)) where 6.25% were neutral (N=5). Majority of the people agreed (N=45) and strongly agreed (N=15) with a total of 75%. While 16.25% of people showed their disagreement (N=13) and 2.5% of people showed strong disagreement (N=2).

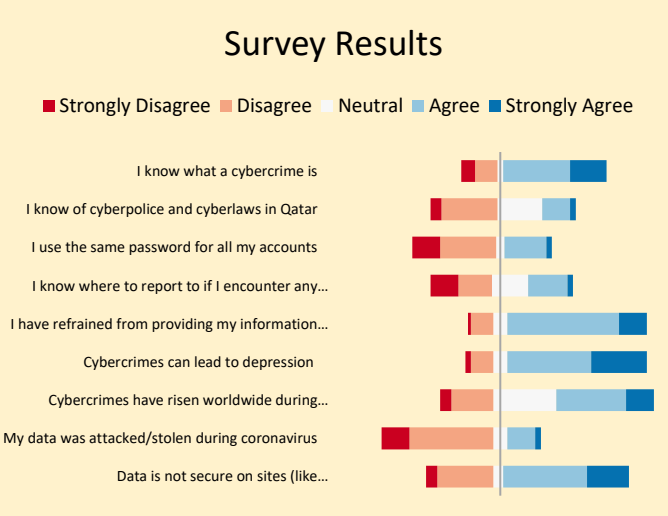

Figure 4. survey results of our research

XI. CONCLUSION

All in all, cybersecurity is a very important field in Qatar, as Qatar develop it and still trying to improve it more and more. Having a strong cybersecurity means that the country is advanced digitally and has a good economy also. Cybersecurity is essential and Qatar opened a new major concentration (cybersecurity). Moreover, Qatar has hosted many cybersecurity conferences and this indicates Qatar interest in this field. Cybersecurity has many pros; however, many cons also exist. Therefore, ethical issues are implied. Such as, cyber-attacks and cyberbullying. Cybersecurity issues in can be solved by several methods. But, a main thing to consider is that internet technology is changing and developing rapidly and that might lead do some difficulties in achieving a very secure system; recently cybersecurity is really challenging and hackers have variety of ways to attack. Qatar associated cybersecurity with many fields such as health and financial field. As well as Qatar ranked it a very high level locally and globally. Globally Qatar ranked in a very high position, Qatar ranked third in cybersecurity index. Similarly, with GCC countries, Qatar is third after KSA and Oman. All this leads to the remarkable development in cybersecurity. This research aims to introduce cyber security in Qatar. In addition to some studies that have been conducted to know the cyber awareness of the population. Analytical studies have shown that cyber awareness is high. But this does not mean that it is not developed, as a percentage of the population still has little information about cybersecurity. Given the importance of security in this era, it is desirable that the state provide some courses or conferences to raise awareness of the importance of cybersecurity and present information about it. Special courses for adults should be different from those for children. Because of different mentalities and children's lack of understanding of technical information and terms. Qatar is improving the technology system in addition to better performance in developing Qatar can sign a contract for cooperation with developed countries in the field of cybersecurity.

References

Al-Dosari, K. (2020). Identification and Prevention of Expected Cybersecurity Threats During 2022 FIFA World Cup in Qatar. *Journal of Poverty, Investment and Development*, 5(1), 49-84. https://iprjb.org/journals/index.php/JPID/article/view/1135/1249

Dean Brown, R. (2019). Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework. *ResearchGate, 4.* 10.29117/irl.2018.0036

Fadlelmula, F. (2020). Undergraduate Student Research on Contemporary Civic Issues in Qatar-Fall 2018 and Spring 2019. *ResearchGate. GlobeEdit.* https://www.researchgate.net/publication/342700986

Foody, M., Samara, M., El Asam, A., Morsi, H., & Khattab, A. (2016) A review of cyberbullying legislation in Qatar: Considerations for policy makers and educators. *International Journal of Law and Psychiatry, 50,* 45-51. 10.1016/j.ijlp.2016.10.013

Mohamed Ali, H. (2021). "Norm Subsidiarity" or "Norm Diffusion"? A Cross-Regional Examination of Norms in ASEAN-GCC Cybersecurity Governance. *The Journal of Intelligence, Conflict, and Warfare. 4(1).* https://doi.org/10.21810/jicw.v4i1.2805

Shires, J. (2018). Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance, 6(2),* 31-40. https://doi.org/10.17645/pag.v6i2.1329

Tabassum, A., Mustafa, M., & AlMaadeed,A. (2018). The Need for a Global Response Against Cybercrime: Qatar as a case study. *ReasearhGate.* 10.1109/ISDFS.2018.8355331

Von Finckenstein, V. (2019). Cybersecurity in the Middle East and North Africa. *Konrad Adenauer Stiftung.* https://www.kas.de/documents/284382/284431/Policy+Paper+on+Cybersecurity+in+the+Middle+East+and+North+Africa.pdf/50199440-b10e-3dea-52ca-c0e3714ebc75?version=1.0&t=1564581818218