Assignment 2.25

Topic: Qatar Cyber Strategies

1. INTRODUCTION:

In aspects of technology, Qatar is rapidly growing its economical activites, as its technology is also growing. The use of technology as a platform for innovation and prosperity. Due to the involvement of Technology in Qatar economy is expanding its cyber space. Cyberspace refers to the interconnected digital environment where computer networks exist, enabling communication, information exchange, and online interaction. This created a new problem to secure this cyber space, as the use of technology also causes the threat of cyberattacks. Qatar countinue to success and growth; therefore, these must be an effective strategy to prevent Qatar cyberspace from these emerging threats to ensure secure economy.

As per Qatar National Cyber Security Strategy (NCSS):

- Secure Qatar's cyberspace with advanced technological measures and collaboration among stakeholders.
- Creating an effective planning that covers todays and future intrest in Qatar Cyberspace.
- Responsibilities for cybersecurity among all individuals and organizations operating in Qatar's cyberspace.

Addressing these points, the cyber security strategies are critical component of Qatar economic state.

2. Importance of Cyber Security to Qatar.

Cyber Security is important to Qatar due to critical factors that involve in national security, economy and in every aspect of life. The use of technology in Financial systems, Energy sectors, Health care industry, Telecommunication infrastructure and in Government activites providing access to information and knowledge that is need to make Qatar more advance and well economical in future. Also enabling to deliver of effective services to customers in Qatar and all around the world, Technology makes it easier to resolve this problem. So ensure the smooth flow of information and achieving high standards of living the security of these technology is important.

KEY INDICATORS OF ICT USE IN QATAR:

- In 2012, 92% of households in the mainstream population had a computer, while 87% of mainstream individuals had a computer.
- In 2012, Internet penetration for mainstream individuals was approximately 88%.

- In 2012, Qatar’s mobile penetration was approximately 100%—one of the highest penetration rates in the world.
- In 2012, 74% of companies in Qatar used computers, including desktops, laptops, and newer tablet technologies; an increase from 64% in 2008.
- In 2012, 66% of businesses in Qatar used the Internet; an increase from 51% in 2008.
- The number of businesses with an ICT security policy increased from 37% in 2010 to 61% in 2012.
- In 2012, skilled ICT professionals represented approximately 2% of Qatar’s total workforce.

Qatar has invested billions of Dollars to improve its country physical infrastructure so to make this investment worth-it, security of this infrastructure should be kept as a critical aspect of its economy.

3. Threats Qatar is facing in Cyber Space:

As the involvement of technology created many new threats, Involvement of ICT uses and connectivity among the business and customers. Qatar's strategic importance and rapid economic development make it a prime target for malicious actors seeking to disrupt its stability and progress through cyberattacks.

Following are some common threats faced by Qatar:

1- **Cyber Crimes:**
Cybercrime is the significant threat to Qatar economy, encompassing various malicious activities such as data breaches, identity theft, and financial fraud. damage to business reputation, and decreased investor confidence. Additionally, the costs associated with cybersecurity measures and recovery efforts further strain economic resources and hinder growth prospects.

2- **Hacktivists**:
Hacktivist represent a critic cybersecurity threat to Qatar's economy, using their technical skills to target government institutions, corporations, or organizations to promote political or social causes. Their activities can disrupt critical services, damage infrastructure, and erode public trust, potentially impacting investor confidence and economic stability.

3- Advanced Persistent Threats (APTs):

(APT) is a stealthy computer network threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state sponsored groups conducting large-scale targeted intrusions for specific goals. APT entities, often state-backed, stealthily breach networks to exhilarate data, conduct espionage, or disrupt operations. Targeting diverse sectors such as government, finance, and industry, they employ traditional espionage techniques and custom malware to achieve their objectives.

4- **Malicious insiders**:
Present a significant cybersecurity threat in Qatar's economic sphere, necessitating robust measures such as strict access controls, continuous monitoring, and comprehensive employee training to mitigate risks and safeguard sensitive data and infrastructure.

4. Challenges:

As Cyber security is critical component in Qatar Economy, it faces many challenges that is needed to be addressed to ensure secure cyber space economy.

1- Limited Cyber Security Expertise:
Qatar struggles with a scarcity of skilled cybersecurity experts, hindering effective threat monitoring and response, thereby risking critical infrastructure and government networks. Insufficient expertise stalls the integration of advanced security measures, amplifying the nation's vulnerability to cyber threats and potential economic distribution.

2- Regulatory and Compliance Challenges:
Regulatory and Compliance challenges in Qatar Cyber space is causing a problem in implementing cyber security practices in industries and other ICT envorment. Qatar's cybersecurity regulatory landscape may be complex and multifaceted, with numerous laws, regulations, and standards governing different aspects of cybersecurity. Navigating this complexity can be challenging for organizations, particularly those operating across multiple sectors or jurisdictions.

3- Public Awareness and Education:
Limited public awareness and education on cybersecurity in Qatar may lead to heightened vulnerability to cyber threats and attacks. Addressing this gap requires targeted initiatives to raise awareness, promote best practices, and empower individuals and organizations to adopt proactive cybersecurity measures.

4- Dependence on External Technologies and Services:
Qatar's dependence on external technologies and services exposes its economy to potential supply chain vulnerabilities and cybersecurity risks. To

mitigate these risks, Qatar needs to prioritize building local capabilities, fostering innovation, and implementing robust oversight mechanisms to ensure the security and integrity of external technologies and services utilized within its infrastructure.

5. <u>Implementing Solutions for Qatar Cyberspace</u>

Focusing on the above challenges faced my Qatar economy the following solutions can be implemented to overcome this problem:

1- **<u>Investment in Cybersecurity Education and Training:</u>**
Qatar should implement the training about Cyber security and education, training, and professional development programs. This create their own workforce that fulfill this requirments. offering scholarships for cybersecurity studies, and collaborating with international institutions to leverage expertise and best practices can be a best solution.

2- **<u>Promotion of Local Cybersecurity Innovation:</u>**
Qatar should promote cyber security envorment at local level educating and motivating local infrastructure, addressing the current problems faced by the country and supporting cybersecurity startups and incubators, and facilitating knowledge exchange and collaboration within the cybersecurity ecosystem.

3- **<u>Public Awareness and Education Campaigns:</u>**
Public awareness is very important because educating individuals businesses, and government entities in Qatar. These campaigns should focus on raising awareness about common cyber threats, promoting best practices for cybersecurity hygiene, and encouraging proactive risk mitigation strategies.

4- **<u>Collaboration and Information Sharing:</u>**
Establishing collaborative frameworks and information-sharing platforms among government agencies, private sector entities, academia, and international partners is essential for effectively combating cyber threats. This involves facilitating the exchange of threat intelligence, best practices, and incident response capabilities to enhance Qatar's cyber resilience and response capabilities.

<u>Conclusion</u>

In conclusion by adopting these approaches, we can Implement cyber security Qatar can strengthen its cyber resilience and safeguard its economy against emerging cyber threats in an increasingly interconnected and digital world. By prioritizing cybersecurity measures and fostering collaboration, Qatar can navigate the evolving digital landscape and emerge as a resilient leader in the global digital economy.

References

1- Tabassum, A., Mustafa, M. S., & Al Maadeed, S. A. (2018, March). The need for a global response against cybercrime: Qatar as a case study. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-6). IEEE.

2- Nasser, A. L. (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.

3- Zubair, M., Unal, D., Al-Ali, A., Reimann, T., & Alinier, G. (2021, September). Cybersecurity for next generation healthcare in Qatar. In Journal of Emergency Medicine, Trauma & Acute Care, Qatar Health 2020 Conference (Vol. 2021, No. 2, p. 41). Qatar: HBKU Press.