ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (88-94), Month: January - March 2021, Available at: www.researchpublish.com

Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies

Abdullah Al Mamun[*1], Jamaludin Bin Ibrahim[2], Sk Mamun Mostofa[3]

[1, 2] Department of Information Technology

[3] Department of Information Science and Library Management

[1, 2, 3] International Islamic University Malaysia, Gombak, Kuala Lumpur, Malaysia

meghmamun25@gmail.com*[1], jamaludinibrahim@iium.edu.my[2], mostofa@du.ac.bd[3]

Abstract: **Technology is an ever-changing expression in the digital age that has increased security risks and forced us to create a cyber-environment. The use of technology in Bangladesh has increased significantly over recent decades. At the same time, it provides the nation with new cyber-space threats and challenges. In order to deal with these challenges in the region, there are many awareness-raising initiatives provided by government and non-government actors. The increasing occurrence of cyber assaults has become a key concern that makes people more afraid of cyber wars than of nuclear weapons and environmental degradation. A troubling degree of comprehension that is not sufficient has been found in this study. A substantial part of the population is unaware of cyber security mechanisms and regulations. The associated organizations, as well as the government, are not even concerned about issues with cybercrime. A major change is required to strengthen cyber security policies and procedures. Moreover, over time, it needs to be supervised and restructured. This pilot study is planned to suggest a systematic investigation into the extent of the awareness of cyber security among Bangladeshi citizens. For this purpose, the article briefly investigates the understanding of cyber security awareness along with the route background strategies in Bangladesh. In order to provide a stable, safer and more productive cyber space at all levels, it proposes recommendations and methods that should be implemented to increase the level of consciousness.**

Keywords: **Cyber Security, Awareness-raising, Strategy, Cyber Security Policy, Bangladesh, Cybercrime.**

I. INTRODUCTION

The rapid growth of and easy accessibility to ICT, coupled with economic progress, has significantly increased the number of first-time users in developing countries. Indeed, the rapid growth in internet users is today taking place in developing nations, especially in Asia and Africa.[1] Cyberspace is an indispensable part of the development of any country. Strong cyber security is essential for states to progress and develop in the technical, social and economic realms. As a result, CCB needs to be incorporated into development projects so that countries can get the help they need to promote their growth and development and protect them.[2]

Bangladesh has achieved economic development with a population of 160 million through the application of science and versatile information and communication technology (ICT) on a land of only about 55,000 square miles and not with many natural resources beneath the soil. It should be noted here that while the industrialized countries of the world have pursued national growth and social welfare opportunities for science and technology, developing countries have fallen behind largely due to various their inadequate knowledge of the potential of science and technology.[3] Progressive advances in the field of ICT have created new possibilities for developing countries are moving forward by intelligently leveraging their potential along the road of growth.

The Ministry of Science, Information and Communication Technology (MoSICT) of Bangladesh has concentrated its focus on contributing to reducing poverty by improving education through the application of ICT among poor people living in rural areas.[4] Education results, productivity and quality are also planned to be improved by adopting a culture of friendly environment and transparency from which the common masses will flourish and contribute positively to nation-building. In order to better develop and promote their products, rural people will be given the availability of the necessary details. Residents at large must be provided with the skills needed to successfully perform their duties. The Government of Bangladesh has taken several steps in recent years to boost scientific and technological research and ICT activities. The services required further collaboration with the international code and systems to be carried out with absolute, utmost commitment by Bangladesh.[5] By forming a high-powered National Task Force on ICT, Biotechnology and the National Council for Science and Technology, the Government has promoted science and ICT and exhibited its commitment to the harmonious growth and innovation of scientific and technological development across the world.

Knowledge is the first line of defence for the security of information systems and networks. Together with society (represented, for example, by non-governmental organizations (NGOs), non-profit organizations (NPOs), universities and private companies), the government of Bangladesh is therefore promoting IT, cyber security awareness and privacy policies in the country. In order to tackle cybercrime increasing awareness among all partners and stakeholders is crucial and yet not sufficient, while, on the other hand, promoting privacy and awareness issues by providing best practices in cyber security to vulnerable populations is essential.[6] These vulnerable groups are: workers of organizations, political, industrial, the private companies; parents and guardians; children and youth, etc. For this reason, the main idea of spreading knowledge is to promote a culture of cyber security that meets the needs of the population affected.

Bangladesh is a country that has been rising rapidly in recent years, especially with regard to telecommunications and information society. The use of Information and Communication Technology (ICT) is dramatically growing, as shown by the State Statistical Office for 2015, with internet access being available to 69.4% of households, while the figure is 93.5% for companies with 10 or more employees. Another important statistic is that internet access is increasing well, through broadband internet connections.[7] This rising use of ICT tends to leave no doubt that the country must in some way update its IT and cyber security environment and skills. Although the government has spent budgets to secure the infrastructure, all it takes is one employee clicking on an incorrect link to compromise the critical data and information system. As a consequence, in the global, organizational and social dimensions of the current period, the security knowledge of end-users is currently a major issue. The danger climate is similarly complex, and many end-users are not aware of the ways in which their individual well-being, their business or the state can be dramatically affected. For this purpose, in building a culture of cyber security and raising awareness by trying to optimize awareness of the weakest security link, which is the human aspect, constructive action should be taken into consideration.[8]

Based on the above information, this paper first discusses the government policy and initiatives under way in terms of awareness raising. Then it offers a summary of the generated campaigns and activities of NGOs, NPOs and schools. Last but not least, in order to protect the weak points in Bangladesh, the article addresses some suggestions on how to create and change cyber and IT security awareness. Finally, the article concludes by describing and presenting feedback on what is in Bangladesh based on awareness and strategy.

II. PROBLEM STATEMENT

Bangladesh is a developing country which is currently undergoing an ICT transformation, is the focus of the article. Bangladesh is now adopting ICT and is greatly expanding the use of ICT and the Internet. They have high hopes for the positive results of their investment, but their benefit has yet to be reaped. In this region, there are developing ICT nations and their communities are emerging online. The study in this paper showed that policymakers in the country need more guidance about how their cyberspace can be secured. They conclude that their condition does not fit the approach used in the current guidelines. A deeper understanding of the cyber security issues in this nation is needed. The problems faced need to be better clarified and the situation analysed for ways to overcome the challenges and where further research is needed.

III. LITERATURE REVIEW

A. Current Status of Cyber Security Awareness in Bangladesh

The National Council for Science and Technology (NCST) has been formed by the Government of Bangladesh to enhance the living standard of the common mass through the extension and implementation of science and technology development activities. The Executive Committee for NCST has also been formed in order to implement the policies formulated by the Council. The recent National Information and Communication Technology Policy (2002) has also provided ICT growth with tremendous potential to capture our share in the multi-billion - dollar software export market, establish effective governance, integrate ICT-related policies, separate allocation of resources for software development projects, to produce world-class ICT professionals.[9]

The vision of this strategy is to create an ICT-driven nation by 2006 that involves a knowledge-based society. In order to achieve this aim, a national ICT infrastructure will be set up to ensure access to knowledge for every citizen in order to facilitate the empowerment of people and enhance democratic values and standards for sustainable economic growth through the use of strategic human resources infrastructure, good governance, e-commerce, banking, public utilities and all kinds of online ICT-enabled services. The national ICT strategy includes, on a priority basis, economic and social growth, the construction of ICT infrastructure, the facilitation of research and innovation in ICT and the development of the ICT industry. (Aziz, A. 2020).[10] It also discussed the importance of hardware industries, e-commerce, e-governance, ICT-related legal issues, the use of ICT in health care, the use of ICT in agriculture to take advantage of rural and agricultural sectors' growth opportunities. The integration of ICT in other areas, such as social welfare, transport and the judicial system, is also highlighted. In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce.[11]This is regarded as the UNCITRAL e-commerce Model Rule. Bangladesh has drawn up an ICT law in line with the UNCITRAL Model Law, which was authorized by the highest authority in February 2005 to stimulate electronic commerce and to contribute to the growth and advancement of information technology.

Rules and specifications for the authentication and acceptance of contracts, forms through electronic means, default rules for the establishment of contracts and the management of the performance of e - contracts are set down in ICT law, the attributes of a genuine electronic document are specified, and the original document provides for the appropriateness of electronic signatures for registration.[12] Furthermore, the Copy Right Law 2000 was revised to include computerized systems. A direct and sustained effort to reduce inequality, strengthen the security of livelihoods, eliminate hunger and malnutrition, and create jobs remains the responsibility of the government. This will call for the generation and screening of all relevant technologies, for their rapid dissemination by networking, and for the assistance of the large, unorganized sectors of economic operation.

The name of the Ministry has been changed from the Ministry of Science and Technology to the Ministry of Science and Information & Communication Technology, recognizing the value of ICT and the immense effect it can have on our daily lives. The obligation for the harmonious development of this industry in Bangladesh has been delegated to the Ministry of Sciences and ICT. The Ministry of Science and ICT is also regulated by the Bangladesh Computer Council (BCC), the main body responsible for promoting all kinds of ICT activities in the country. The creation of science and ICT relies on the growth of the telecommunications industry. Owing to a lack of deregulation and free competition, this sector is still under developed. In 2002, the Bangladesh Telecommunication Regulatory Commission (BTRC) was established as an independent telecommunications regulatory authority.[13]

B. Cyber security Perception Stability in Bangladesh

Many developing countries, such as Bangladesh, have restrictions on access to information, and access to it is not cost-effective in terms of the insufficiency of existing infrastructure and the lack of appropriate education. The obstacles are tackled by the absence of an integrated information protection infrastructure and cyber security education. Cooperation, partnership and security investment are also required, which also generates a culture of security standards to ensure safety concerns.[14] Trust is vital, as in business or any operations, and trust can be obtained when the professionals believe that the agreement is protected. Consequently, protection from a business viewpoint must be seen as a strategic business partner, not as a cost enabler.

The lack of an appropriate framework for information security is one of our challenges, and cyber security awareness is also one of the most important issues. As significant next steps for raising awareness and the availability of necessary intelligence, Bangladesh is preparing, as well as the development of security standards.[15] Further implementation processes related to the security requirements of information systems are needed. In order to realize these objectives, global cooperation is important. We also recognize that research and development is more important for the Information Security System Program, while at the same time we need to play a leading role in a successful program leading to understanding and cooperation, fostering risk management methods and best practices, and pursuing standardization initiatives, thereby enhancing the worldwide understanding of technology.[16]

Bangladesh is aware that information security is an important enabler for business and is crucial for more cooperation between countries and across industries, and it is appropriate to look for plans to manage effective public-private partnerships.[17] In order to safeguard cyber security, there is an urgent need to implement cybercrime regulations. Additional cyber-crime policy program and enforcement awareness development and training initiatives throughout the nation are also required. The country's strategies should also be secured by security controls, trust points and other self-regulatory steps for the development of goods and the provision of services and the implementation of the necessary measures to create consumer confidence.

C. Recent Cyber Attacks in Bangladesh

The occurrences of cyber-attacks continue to increase at various commercial and service-providing outlets across the country while taking multiple safety measures. As the country achieved a significant progress particularly on socioeconomic front in the era of digital technology, the number of cyber related incidents is also increasing.[18] As a result of the jump in crimes related to information technology, the topic of cyber security has become a matter of great concern for most important public and private organizations.

According to the state-run Bangladesh e-Government Computer Incident Response Team (BGD e-Gov. CIRT) under the Ministry of Posts, Telecommunications and Information Technology, the incidents registered by the organization rose to 870 in 2018 from 683 in 2017.[19] The figure was 379 in 2016. Vulnerability accounts for 63.2% of attacks, 5.7% of attack or hacking, 22.5% of malicious code, 4.5% of offensive material, and the remainder includes fraud, attempted invasion, request for service, identity security, and others. However, since the state-owned special unit does not disclose such injuries to a large number of commercial or service-providing sources, the real number of attacks will be much higher, insiders said. The government founded BGD e-Gov. CIRT under the Bangladesh Computer Council (BCC) only after the Bangladesh Bank's reserve heist incident.[20] To further combat any such fatal intrusions, it was established. The Bangladesh Bank has warned all banks of a new cyber assault by a North Korean-based hacker group, calling for extra security measures to be taken. The warning came after a cautionary alarm from the US Federal Reserve Bank was released by the central bank two weeks ago, according to a source from the Bangladesh Bank.[21] Some banks with a large digital banking network have, according to some bankers, reduced their online operations following the warning. "We got a warning notice about a hacking group based in North Korea from the central bank about 10 days ago," said Syed Mahbubur Rahman, managing director of Mutual Trust Bank. He said a hacking group had been trying to infiltrate the US banking system recently. As a result, they have sent all central banks a letter to take precautionary measures. "In order to stop cyber-attacks from all aspects of the IT system, we have taken security precautions," he stated.

In order to mitigate the cyber-attack, the Dutch-Bangladesh Bank, which has the country's largest network of ATM booths, temporarily suspended booth transactions after 11 pm, the bank's source said.[22]The cyber-attack warning came at a time when the country's banks are strongly expanding their digital banking network in the midst of an epidemic. Bangladesh Bank experienced the greatest cyber heist earlier in February 2016, taking $81 million from its New York Fed foreign exchange reserve fund. The role of the North Korea-based hacker community in this heist was identified by a FED investigation. Since then, the central bank has attempted to pay back the stolen money. In the midst of the Covid-19 pandemic, the country's online banking services have been growing as customers pursue online services to shield themselves from the virus. According to data from the central bank, payments via Internet banking jumped 12.6 percent in June 2020. In March, when the first coronavirus case was identified by the government, online banking activities were Tk6, core 588. The monthly transactions had increased to Core Tk7, 421 by June of this year. In the midst of an epidemic of disease, this increase in online banking is the result of a mega change in the banking sector from conventional banking to digital banking.[23] Many Bangladeshi banks, however, have significantly increased their digital networks, and security concerns remain high here owing to a shortage of skilled labour and lower spending on IT security, the bankers stated.

IV. METHODOLOGY

Methodology can be stated as a set of procedures followed for carrying out any systematic investigation.[24]The research methodology adopted for the study is investigative and also based on a comprehensive review of literature, computation of secondary sources of information. This research involves the collection of the necessary information from the identified records relating to the intended subject. Since the current study examines the literature and resources such as cyber security after identifying the existence of interactions between facilitators and systems. Qualitative research will therefore be pursued in this article to analyse and come to an understanding of the awareness and policy of Bangladesh's cyber security. In summary, a research analysis results in recommendations for different industries and basic regulations. These recommendations are: the need to make amendments to some of the parts of the regulations reviewed or to implement new legislation to ensure the confidentiality of people when their private data is collected, stored, processed and transmitted and to provide end-users with ongoing awareness-raising training on the security of information and personal data. This activity will help nations to acquire the necessary resources and skills to build a robust infrastructure and technology to achieve the required level of cyberspace security needed.

V. RECOMMENDATIONS OF MEASURES TO INCREASE CYBER SECURITY AWARENESS IN BANGLADESH

To effectively resolve cyber threats and strengthen cyber security, cyber protection needs a multi-stakeholder strategy. Intra-state and international collaboration is also required, in addition to intra-national cooperation (public, private sectors, ISPs, etc.), due to the global nature of cyberspace.[25] Thus, no nation will remain safe from cyber-attacks. Awareness of cyber security will significantly reduce the severity of cyber-attacks. The awareness of its violations has not evolved in the same way as the internet is rising. The measures that need to be taken to raise awareness among the masses of citizens and government employees are addressed in this policy section. The introduction of guidelines, if complied with, would help mitigate cyber security risk to the national cyber space when the cyber security policy is developed or updated.[26]

- Evaluation of current technology legal frameworks to assess if they are criminalized in an acceptable manner to count as a case of deliberately committed misuse of telecommunications and computer networks. Sooner or later, this would help to facilitate the investigation of cybercrimes.

- Countries should properly recognize issues related to high-tech-related offences if discussions on mutual agreements are conducted.

- Countries must establish the appropriate protocols necessary to acquire traffic data from communication channels. Strategies should be developed to ensure that the expedition is in the process of international data transmission.

- The very first step towards strengthening our cyber security is to create regulations and then implement them. To make this possible, governments need proper legislative approval. This includes the establishment of cyber security organizations (e.g., the National Cyber Security Council).

- Focus on protecting national cyberspace as a whole and upholding the civil rights of internet users, rather than submitting a strategy to the security of essential properties alone.

- In the paper, the initiative to focus on protecting cyberspace from possible attacks such as smartphones, cloud computing, big data, etc.

- Incorporate the concept of agility by subjecting the plan to periodic evaluations and market feedback to stay competitive with technical advancements and complexity in rising cyber threats.

- Require feedback on the national cyber security policy or management strategies from all relevant stakeholders; government, military, telecommunications companies, financial institutions, judiciary, civil society, religious groups, cyber security specialists etc.

- Help the initiative by illustrating a detailed cyber management plan with properly specified stakeholders, officials, transparency, objectives, investments, results, etc.

- Demonstrate the necessity, in the plan, to change the national legal framework to handle efficiently with cybercriminals and suspects.

- Suggest additional programs for education and training, cyber security toolkit, etc. in practice self-training for individuals, and the cyber consciousness of the nation.

- Provide guidance on enhancing private-public collaborations to ensure effective implementation of cyber resilience of the national cyberspace.

VI. CONCLUSION

In the age of digital transformation, cyber security is a global concern. This study showed that the level of awareness of cyber security among the citizens of Bangladesh is at a vulnerable stage and fast action is needed to speed up the level of awareness of cyber security. If people had previous knowledge of cyber security weaknesses, they would end up finding ways to defend themselves. In this regard, Bangladesh can follow the paths of developed countries to mitigate the risk of vulnerability. We have some specific ideas being suggested. Knowledge and understanding is the main concept of keeping information secure from burglars. This concept is often pointed to as an understanding of cyber security that can be accomplished in many forms. In order to increase the level of awareness for government officials, the Government of Bangladesh should conduct cyber security awareness and threat assessment programs at government offices at an orderly interval on an ongoing basis. The regular implementation by private companies of similar initiatives to mitigate security threats caused by internal workers should be enforced by the government. The new strategy encourages organizations to invest in an organization-wide data security budget statement that includes all their cyber-related operations. Another effective instrument is the integration of cyber security awareness into school and college education programs. It will make our students aware of cyber security issues, and in turn, students would pursue higher education in cyber security and enter cyber security career paths that have growing ambitions in the worldwide job market. Furthermore, multiple cyber security initiatives, especially for children and students in academia, play an important role in raising awareness of cyber security. These initiative subjects can vary in versatile cyber security problems with different lengths of time.

REFERENCES

[1] Wintner, S., Tadić, M., & Babych, B. (2014, April). Proceedings of the Demonstrations at the 14th Conference of the European Chapter of the Association for Computational Linguistics.

[2] Muller, L. P. (2015). Cyber Security Capacity Building in Developing Countries. Norwegian Institute for International Affairs (NUPI).

[3] Team, C. (n.d.). Government of Bangladesh Information Security Manual (GoBISM) has been published. Retrieved November 04, 2020, from: https://www.cirt.gov.bd/government-of-bangladeshinformation-security-manual-gobism-has-been-published/

[4] Bangladesh Ministry of Science, Information, and Communication Technology (MoSICT). Retrieved November 04, 2020, from: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN026243.pdf

[5] National Initiative for Cyber security Careers and Studies: Integrating Cyber security into the Classroom. [Online]. Retrieved November 07, 2020, from: https://niccs.us-cert.gov/formal-education/integratingcybersecurity-classroom.

[6] Ahmed, N., Kulsum, U., Azad, M. I. B., Momtaz, A. Z., Haque, M. E., & Rahman, M. S. (2017, December). Cyber security awareness survey: An analysis from Bangladesh perspective. In 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) (pp. 788-791). IEEE.

[7] Tasevski, P. (2016). IT AND CYBER SECURITY AWARENESS-RAISING CAMPAIGNS. Information & Security, 34(1), 7-22.

[8] Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). An exploration of the design features of phishing attacks. Information Assurance, Security and Privacy Services, 4(29), 178-199.

[9] National Cyber Security Index. [Online]. Retrieved November 08, 2020, from: https://ega.ee/project/national-cyber-security-index/.

[10] Aziz, A. (2020). Digital inclusion challenges in Bangladesh: The case of the National ICT Policy. Contemporary South Asia, 28(3), 304-319.

[11] Overby, A. B. (1999). Will Cyber law be uniform--an introduction to the uncitral model law on electronic commerce, Tul. J. Int'l & Comp. L., 7, 219.

[12] Bangladesh Law Digest: [Online]. Retrieved November 08, 2020, from: http://bdlawdigest.org/cyber-crimes-and-cyber-laws-in-bangladesh.html.

[13] Bangladesh Internet Subscriber: [Online]. Retrieved November 08, 2020 from: http://www.btrc.gov.bd/content/internet-subscribersbangladesh-june-2018.

[14] Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

[15] Ahmed, N., Islam, M. R., Kulsum, U., Islam, M. R., Haque, M. E., & Rahman, M. S. (2019, September). Demographic Factors of Cyber security Awareness in Bangladesh. In 2019 5th International Conference on Advances in Electrical Engineering (ICAEE) (pp. 685-690). IEEE.

[16] Siddique, N. A. (2019). Framework for the mobilization of cyber security and risk mitigation of financial organizations in Bangladesh: a case study.

[17] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.

[18] Haque, A. K. M. (2019). Need for Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh–Hype or Reality? International Journal of Managing Information Technology (IJMIT) Vol, 11.

[19] BGD e-GOV CIRT's mission is to support government efforts to develop and amplify ICT programs has been published [Online]. Retrieved November 10, 2020, from: https://www.cybersecurityintelligence.com/bgd-e--gov-cirt-3002.html

[20] Bangladesh Computer Council (BCC) Cyber Security related services include cyber security incident handling and digital forensics has been published [Online]. Retrieved November 10, 2020, from: https://www.cybersecurityintelligence.com/bangladesh-computer-council-bcc-4752.html

[21] Central Bank of Bangladesh, has been published [Online]. Retrieved November 10, 2020, from: https://www.bb.org.bd/en/index.php

[22] The Daily Star, Bangladesh news: [Online]. Retrieved November 10, 2020, from: https://www.thedailystar.net/frontpage/9-dutch-bangla-bank-atms-victim-of-international-fraud-gang-1755148

[23] The Business Standard, has been published [Online]. Retrieved November 10, 2020, from: https://tbsnews.net/economy/banking/pandemic-boosts-internet-banking-

[24] Walia, P. K., & Siddiqui, S. (2013). A comparative analysis of Library and Information Science post graduate education in India and UK. Library Philosophy and Practice, 1.

[25] Basamh, S. S., Qudaih, H. A., & Ibrahim, J. B. (2014). An Overview on cyber security awareness in Muslim countries. International Journal of Information and Communication Technology, 4(1).

[26] Berenskoetter, F. S. (2005). Mapping the mind gap: A comparison of US and European security strategies. Security dialogue, 36(1), 71-92.