Journal of Computer Science and Technology Studies (JCSTS)
www.jcsts.one
2709-104X

Research Article

Cyber Security and Approaches of Institutions: A study on private institutions of Banani and Dhanmondi Thana area, Dhaka

Shaira Matin[1] and Md. Monwarul Islam*[2]
[1]*Assistant Professor, American International University Bangladesh (AIUB), Dhaka*
[2]*Head of Business Intelligence, RM Group, Bangladesh.*
Corresponding Author: Md. Monwarul Islam, E-mail: manamigc1994@gmail.com

ARTICLE INFO

Article History
Received: October 21, 2019
Accepted: December 22, 2019
Volume: 1
Issue: 1

KEYWORDS

Private institutions, cyber security, limited resources

ABSTRACT

Cyber security is considered as business issue more than a technical issue. The term widely used in Bangladesh since last decade. Dealing with information made our life resourceful, and risky at the same time. Cyber security and private institutions keep a silent but significant relation around Bangladesh. Corporate offices, public and private organizations have dealing with private cyber institutions to develop, design and monitor the respective websites. This paper has conducted study on those private institutions of Dhanmondi and Banani Thana administrative areas. The study found the diversity of working area of private institutions and limited resources to continue the activity. International collaboration and support from government can increase the strength of private cyber institutions and consider their performance as the potential resource for the cyber world.

1. Introduction

The concern of cyber security has been increase since the development of Digital Infrastructure around the country. The Vision 2021 is giving high priority to build a networked society in Bangladesh where Information Communication Technologies were thought to be a key enabler by the current government (A2I Programme, 2011). The overarching development agenda has made progress from top to bottom level; from District level to Union Administration level. Apart from the thought of conventional security system, cyber security has taken a new place after the cyber-attacks in financial and organizational areas. Organizational and financial websites keep critical information that could hampered the strategic progress of that particular organization. Cyber security and cyber-crime both has similarity in context of internet base security studies and prevention of crime.

According to Kaspersky (2019), Cyber security to some extent known as electronic information security or information technology security, is a practice against malicious attacks to protect computers, servers, systems, networks, and data.

Cyber-crime is defined by the Council of Europe, “Any criminal offense committed against or with the help of a computer network is known as Cyber-crime” (Kamruzzaman et al., 2016). The definition may change a little as new devices are taken places and the users of internet are growing faster. According to BTRC, the number of internet subscriber* in Bangladesh has reached 96.199 million in the month of June, 2019. Among them, 90.409 million subscribers are using mobile internet (Btrc.gov.bd., 2019). The expanding rate of internet users and services are creating new challenges to the cyber security of Bangladesh. The lack of efficient response became a great concern to the holders of Critical Information Infrastructures (CCI) and local internet users.

Different organizations and institutions, irrespective to their size and forms, have become increasingly dependent on information technology (UNODC, 2019). Especially, banking and financial sectors are getting involved in web based money transaction to make their services friendlier to the customers. Financial inclusion is another factor that makes banking sectors dependent on internet based banking or e-banking. Not only the financial sectors but also academic institutions are involving in web site based communications. To fulfill the long term agenda of the present government, all sectors have been brought under internet based communication network, which ensures the objected development in a large scale. At the same time, cyber security has become a great concern with increasing number of internet users.

More than two decades ago, there is a link found between computer technology and terrorism, and it has been a theme in the United States national security literature (Cavelty, 2008). Now, the threat has outbreak around the globe. The newly adopted Digital Security Act, 2018, a provision to handle or prevent digital security issues in Bangladesh, has described punishment for committing cyber terrorism. As the involvement of internet in national and international communications have spread so fast, the threat has been raised keeping the pace with this internet based development. So far, the connection between cyber-crime and terrorism have been described by different groups (Sofear & Goodman, 2000), concern with the topic with topics such as freedom of speech and internet censorship (Glandman, 1998; Weiman, 2004; Cavelty, 2008). In this paper, institutions mean cyber institutions that deal with web development, management, training and to some extent provide functional security. Institutions play a key role to monitor and manage cyber security issues. There are both international and national institutions involved in the cyber security issues, the collaboration of these institutions are helping worldwide to fight against cyber-crime. Choucri et al., (2014) highlighted international institutional theory and an empirical “census” of the institutions in place for cyber security, to design a new mechanism in response of cyber threat. But in this paper, national institutions are emphasized to understand their strength in response of cyber threat.

In Bangladesh, institutions are often hired by organizations to maintain website and cyber security issues. In this paper a semi-structured questionnaire interview conducted on some key institutions which are usually perform web base management works. Our focus is to know their strength and weakness while dealing with critical information infrastructure.

Writing on security issues requires specific understand that sometime raise question to the background of the author. But identification of the problem and working on it to find the approximate solution can be a way to understand a present context like the contribution of private institutions in the world of cyber security. Limited works found in this topic and sometime it is challenging to get information from private institutions. This study allows private institutions to take part in participatory role where contemporary security issues reflected along with the exercise of cyber security in Bangladesh.

1.1 Problem statement

Cyber institutions in the commercial areas play a key in developing business and communication. As the metropolitan (Dhaka) is on the way to become a megacity by 2030, it has some potential impact on the systems and services of the city. The biggest concern silently raises apart from the view of conventional security strategy. Many scholars especially Sofear and Goodman, (2000); Finn, (2007); Denning, (1999); stated about electronic security issues, at the same time they mention these securities should get same priority as like as the conventional security issues.

Nowadays, Bangladesh has wide ranging dependence on private cyber institutions or agencies; to develop website, internet solution, ucam and critical information infrastructure (CCI) security. But systematic developments are not keeping pace with the mainstream digital development agenda and lack of integrating approaches are predominant in the private cyber institutions. The functional profile of private cyber institutions need to observe to identify the crisis in the security sector.

1.2 Objectives

The aim of the study is to understand the condition of cyber security with the lens of private institutions in Dhaka. Following objectives will assist to achieve the goal of the study

The primary objective is to identify the functional approach of institutions in response of cyber threat.

The secondary objective is to identify the perception of professionals to handle non-technical challenges to provide security services.

3. Literature Review

The term cyber security can be divided into two words, ‘cyber’ and ‘security’; which helps to make a clear understanding on cyber security and its function. According to Oxford Learner Dictionary, the word *cyber* means connected with electronic communication networks, especially the internet. On the other hand, *security* defines the activities involved in protecting something or individual from a particular threat. In this paper, we will discuss cyber security, web base cyber-crimes and activities of key institutions.

Stating a ‘security problem’ while simultaneously address something as not has significant consequences in that it endows ‘the problem’ with a status and priority that ‘non-security’ problem do not have (Hansen & Nissenbaum, 2009). The conventional security studies do not include cyber security, for an example the broadly conceived text book, Contemporary Security Studies, edited by Alan Collins, insert no entries “cyber security”, “critical infrastructure”, “information security”, “computer”, or “networks” (Collins, 2007). Some security studies scholars address cyber-related themes by employing, “adjacent concepts”, “cyber-war” (Der Derian, 1992; Arquilla & Ronefeldt, 1993), “netwar” and “network security” (Arquilla & Ronefeldt, 1993, 2001; Deibert & Stein, 2002; Der Derian, 2003), “ critical infrastructure protection” (Bendrath, 2003), “information security” and “information warfare” (Denning, 1999; Deibert, 2003; Der Derian, 2003; Latham, 2003)-terms that overlap, but also have significant meanings that separate them from cyber security (Hansen & Nissenbaum, 2009).

The concept of cyber security has wide ranging dimensions, from business to mobile computing and it has divide in some categories; Network security, application security, information security, operational security, disaster recovery and business continuity and end user education.

Bangladesh requires jointly support from reliable physical and information communication technologies, to ensure services like communications, emergency services, energy, finance, food, government, health, transport and water (GoB, 2015). The cyber security has given priority to the national level especially, to ensure reliable functioning of digital infrastructure or Critical Information Infrastructure (CCI) to deliver services and to conduct business. A strategical framework has published by the Government of Bangladesh in 2015, named “The National Cyber Security Strategy of Bangladesh”. The document showed a framework that includes cognizant and shared nature of vulnerabilities and strategies require for public-private partnership to fix potential vulnerability of both public and private owned critical infrastructures in banking, utilities and telecommunications sectors against cyber-attacks.

4. Legal Approaches of the Government of Bangladesh to deal Cyber Security

Dhaka Metropolitan Police (DMP): Dhaka Metropolitan Police (DMP) conducts their cyber-crime and cyber patrolling activity from the unit of Counter Terrorism and Transnational Crime (CTTC). This unit also assist other units regarding their mentioned activities in terms of providing terror surveillance.

Ministry of Posts, Telecommunication and Information Technology: The ministry is responsible for communication plan, internet and telecommunication services around the country. The ministry is divided into two divisions; one is Post and Telecommunication Division and another is Information Communication Technology (ICT) Division. ICT division takes care of cyber security issues.

Digital Security Act, 2018: The act made to focusing on National Digital Security and enact laws regarding Digital crime identification, prevention, suppression, trial and other related matters. Chapter 6 of the act describe *Crime and Punishment* criteria. Among them separate provision and punishment has described for different digital crimes. For example; Punishment for Illegal Entrance in Critical Information Infrastructure (CII), Illegal Entrance in Computer and Digital devices, computer system and Punishment, Damage of computer, computer system etc., and punishment, Offense related to Computer Source Code Change and Punishment, Punishment for any propaganda or campaign against Liberation War, Cognition of Liberation War, Father of the Nation, National Anthem or Flag.

Bangladesh Telecommunication Regulatory Commission (BTRC): Under the Bangladesh Telecommunication Regulatory Act-2001, Bangladesh Telecommunication Regulatory Commission (BTRC) established in 2002. BTRC is the responsible authority of Bangladesh Government which provide license and related access permission to the private institutions to carry on business around the country. BTRC also provide license to private telecommunication company and broad band service providers. BTRC has control on internet services and telecommunication connections around the country. BTRC play a pivotal role in cyber security of Bangladesh context.

5. Methodology

Research Design and Evaluation of the topic:

A group of professionals and academician are selected for the evaluation of the topic. With the help of professionals from the leading Information Technology firms and academicians, a checklist and semi structured questionnaire prepared for the cyber institutions.

5.1 Pilot Survey and Study Area

A pilot survey has conducted on 50 randomly selected institutions of Banani and Dhanmondi Thana administrative area. The pilot survey has conducted to select one key personnel from each institution who has taken part in the study. Based on their willingness to participate in the study and also professional experience to serve both individual and organizational cyber issues, we selected 10 institutions. Among them 5 institutions were taken from Banani and rest 5 institutions were taken from Dhanmondi area.

5.2 Key Informant Interview

One key personnel having five years working experience in the field of cyber security with the private institution or the Executive Engineer of cyber monitoring and problem solving cell was selected for the questionnaire interview from each institution. Based on their willingness to participate in the interview, a questionnaire form send to those institutions to know their approach to cyber security.

6. Result and Discussion

The questionnaire forms of both Banani and Dhanmondi areas were compiled. The total number of questionnaire form is 10. The number of total questionnaire form converted to 100 percent to get better view.

6.1 Activities of selected institutions

From the primary data through key informant interview, it has found that 30% institutions involve in website management, 30% institutions involve in web design, 30% institutions provide cyber security services and last 10% institution provide cyber training.

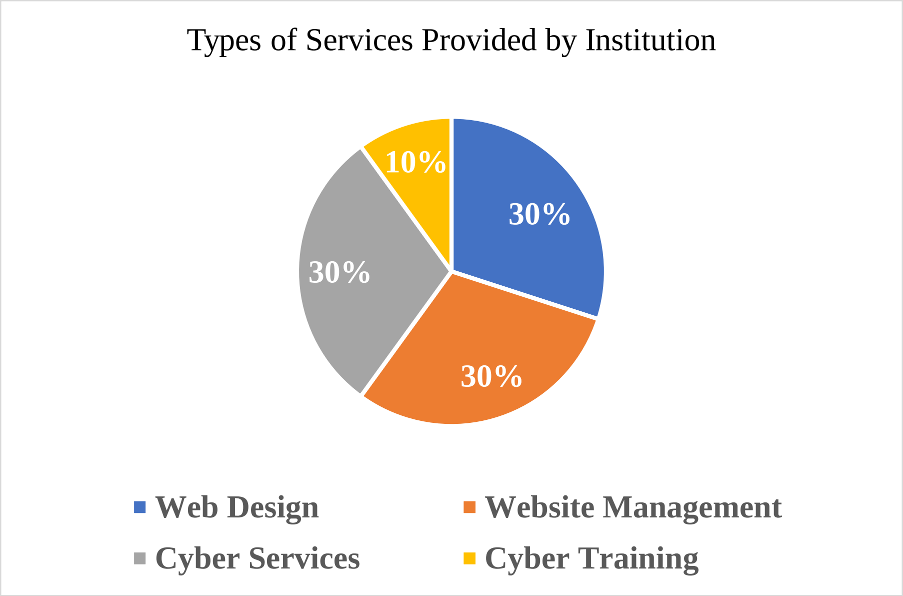

Figure 3.1 Types of services provided by institutions. *Source: Primary data*

6.2 Security issues

Among 10 institutions, 65% marked organizational web hacking found in recent times, where e-mail hacking is second (20%) and Facebook hacking is third (10%) accordingly in terms of recent security issues. Rest 5% cases are found for unauthorized access to USB drive, personal computer and mobile phone. Most significantly organizational or official website hacking is found in financial and academic sectors.

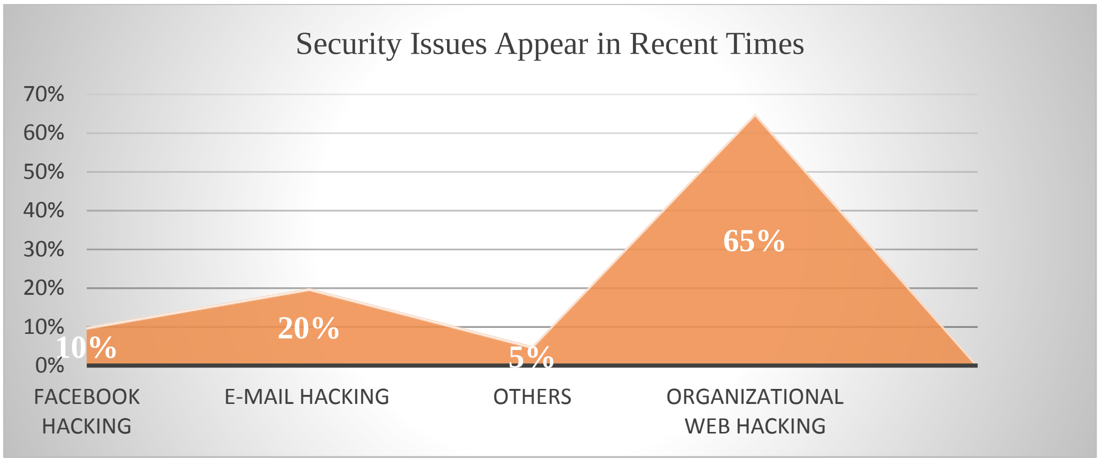

Figure 3.2 Security issues appear in recent times. *Source: Primary data*

6.3 Existence of response system

Only 10% institution have their response system, where they have proper surveillance and response system for any unwanted event or unauthorized access. That particular institution has its own proactive system which does not allow any unauthorized access to their website management system. Rest 90% institution do not have response system to defend unauthorized access to web or system. These institutions were solving affected computers or website based issues but they do not have any prepared system to defend any occurrence before happening.

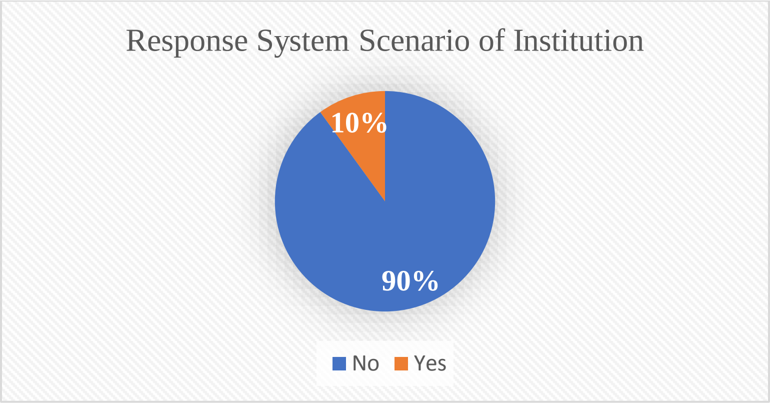

Figure 3.3 Response system scenario of privet institutions *Source: Primary data*

6.4 Cyber Insecurities

From cyber institutions it came to know that cyber insecurities mostly arise with 3 predominant reasons. Most of the institutions claim that the prevalence of cyber bullying (40%) is one of the major reasons behind cyber insecurities. It has to be mentioned that, individual cyber insecurities are mostly arising with cyber bullying. Organizational websites are affected by phishing link (30%). Advertise links are highly suspected for cyber insecurities, 30% respondents agreed that it is infectious to both individual and organizational websites.

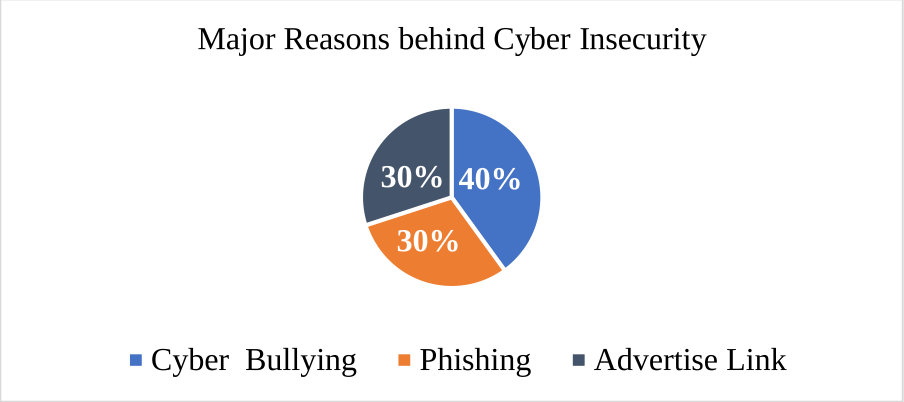

Figure 3.4 Major reasons behind cyber insecurity *Source: Primary data*

6.5 Training for advance cyber security

Only 30% institution's member have received training on cyber security from ICT division of the Ministry of Post, Telecommunication and Information Technology. Rest 70% institution's member did not received training on cyber security from the following ministry. These institutions indicate unknown reasons behind not attending in the government led training programme.

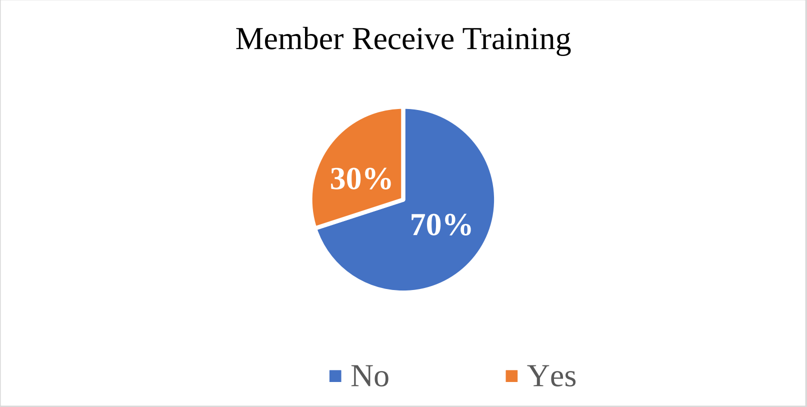

Figure 3.5 Percentage of institutions receive training from government Source*: Primary data*

6.6 Percentage of awareness on cyber security legislation

The awareness level of the institution about new *Digital Security Act-2018*, and other legislations (Information Technology Act-2006, Information Technology Act-2009 (Amended), Information Technology Act-2013 (Amended)) found in the figure 3.6. Among them 40% institutions know about abovementioned legislations of cyber security, and 40% institutions did not know about these legal forms. 20% institutions did not answer the question.

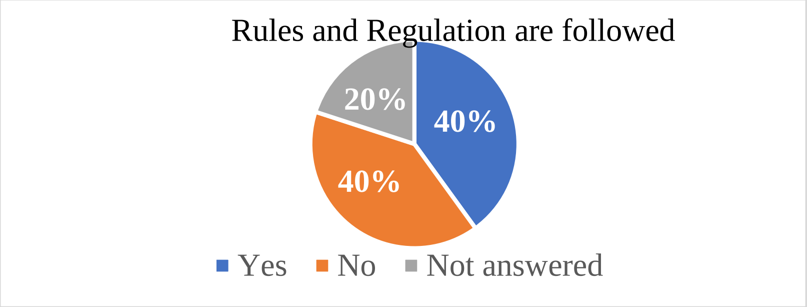

Figure 3.6 Percentage of institutions follow rules and regulations

Source: Primary data

6.7 Knowledge about National Cyber Security Strategic Framework- 2015

Key respondents of selected institutes were asked about National Strategic Framework on Cyber Security-2015. 70% respondents did not know about the strategic framework (Fig. 3.7). 30% respondents know about it but the functional approach of the framework is fully unknown to them. 80% institutes describe the reason behind not knowing about the framework is, the lack of campaign of the framework among Information Technologist or cyber security providers. 20% institute did not answer this question. From the perception of key respondents, 80% thought that there is no effectivity of the framework in cyber security. But rest 20% agreed with effectivity of the framework to redesign cyber security policy and act.

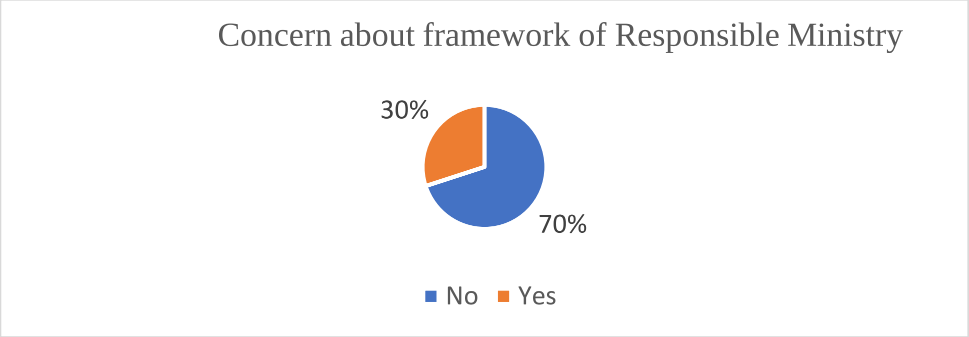

Figure 3.7 Percentage of institutions concern about cyber security framework.

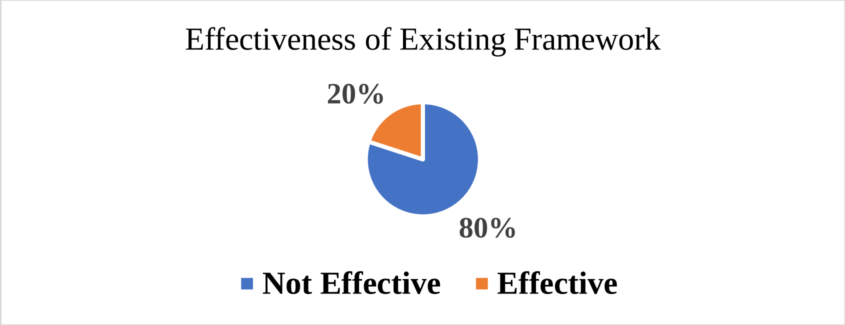

Figure: 3.8 Effectiveness of existing framework *Source: Primary data*

6.8 Collaborating perception to deal cyber issues:

80% of the total institute have individual capacity to deal with cyber issues on regular context. 20% institute need help from other institutions or government to solve cyber issues. For a major cyber issue, 60% institute agree to have collaborating approach to solve the problem, rest 40% institute said they were not agreed because of some business or legal purposes.

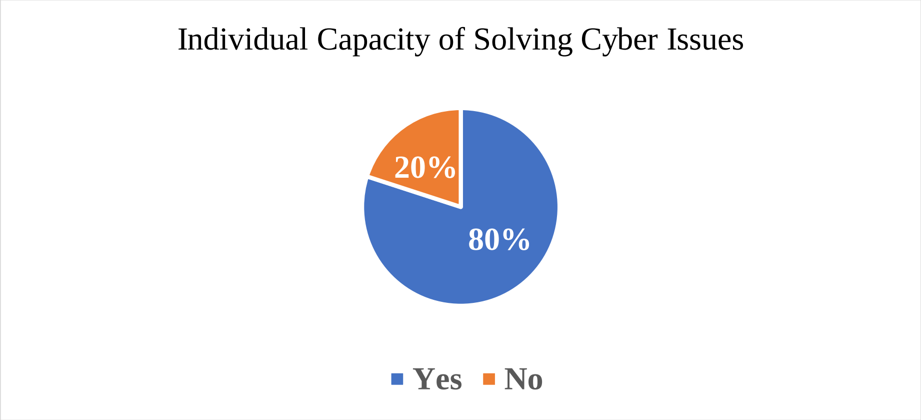

Figure: 3.9 Individual capacity to cyber issues *Source: Primary data*

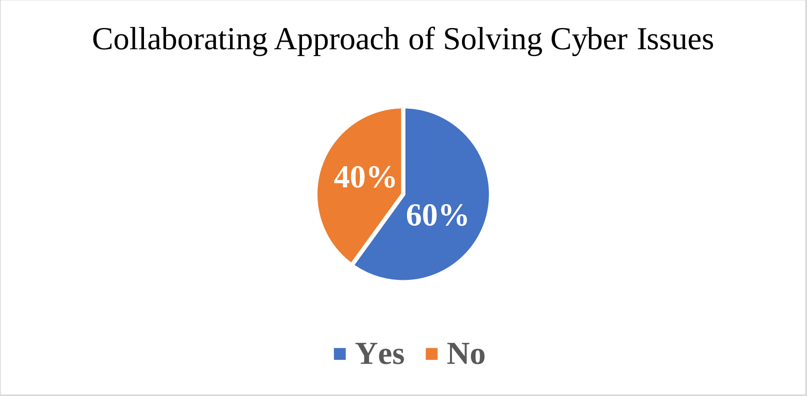

Figure 3.10 Collaborating approach to solve cyber issues *Source: Primary data*

7. Discussion

Selected institutions of Banani and Dhanmondi area provide services to more than 150 organizations and 5 financial organizations or banks. The strength and capacity of these private institutions have become a great concern in context of cyber security. Apart from controlling regular access or technical problems, monitoring unauthorized access is a prime concern for these institutions especially in financial organizations or agencies where critical information lies along with high mobility. Number of initiatives have been taken by the Ministry of Post, Telecommunication and Information Technology to control the prevalence of cyber-crime and ensure cyber security to the door of the households. But focuses on private institutions are not yet significant because business oriented goals and not willing to update newer security protocols. As a result, new security issues may appear and affect the information system or database.

7.1 Co-operative approach

Having individual capacity to deal with present requirements does not mean that particular institutes is well prepared for future cyber risk. ICT division of the concern ministry arrange seminars and workshop on cyber security campaign and enhance of the capacity. The participation of private institutions is not notable. As a result, a gap between public and private institutions found in problem sharing and solving.

7.2 Lack of response system

Figure 3.3 shows, only 10% institutions have own response system to alarm any uncertain event. The system allows to shut down the activity of related website and leave a message for the website administration. Individual security issues require instant solution rather to install a response system. In case of organization security issues, institutions took long time to understand the problem after that thinking about permanent solution or installing response system. Understanding present security issues, a response system needed to design which is suggested by all private cyber institutions. On the other hand, phishing advertise links need to identify and eliminate their sources. Some institutions suggested that, Government can take a holistic approach to control the prevalence of cyber issues. Digital Security Act-2018 is an example of such approach but it need to be more technical and effective to address cyber security issues.

7.3 The exercise of private institutions in response of cyber threat

Private institutions play more reactive role than proactive approach. Within the key informant interview session, it came to know about their response and activities while solving a cyber-security issues. Selected private institutions were dealing with 3 predominant tasks which are Website monitoring and maintenance, Cyber services or solutions and Website design and development.

Website monitoring and maintenance: Institutions which are involve in website monitoring and maintenance have long deal with public and private organizations. Organizations usually make a contract with cyber institutions for a certain time period and these institutions provide 24/7 services to organizational websites. Cyber security is a prime concern for these institutions as they are responsible for all issue regarding the websites of the organization. Cyber institutions are also responsible for any misconduct and they have to ensure proper services within the shortest possible time. Figure 3.2 shows the frequency of organizational web hacking is quite higher than other cyber insecurities.

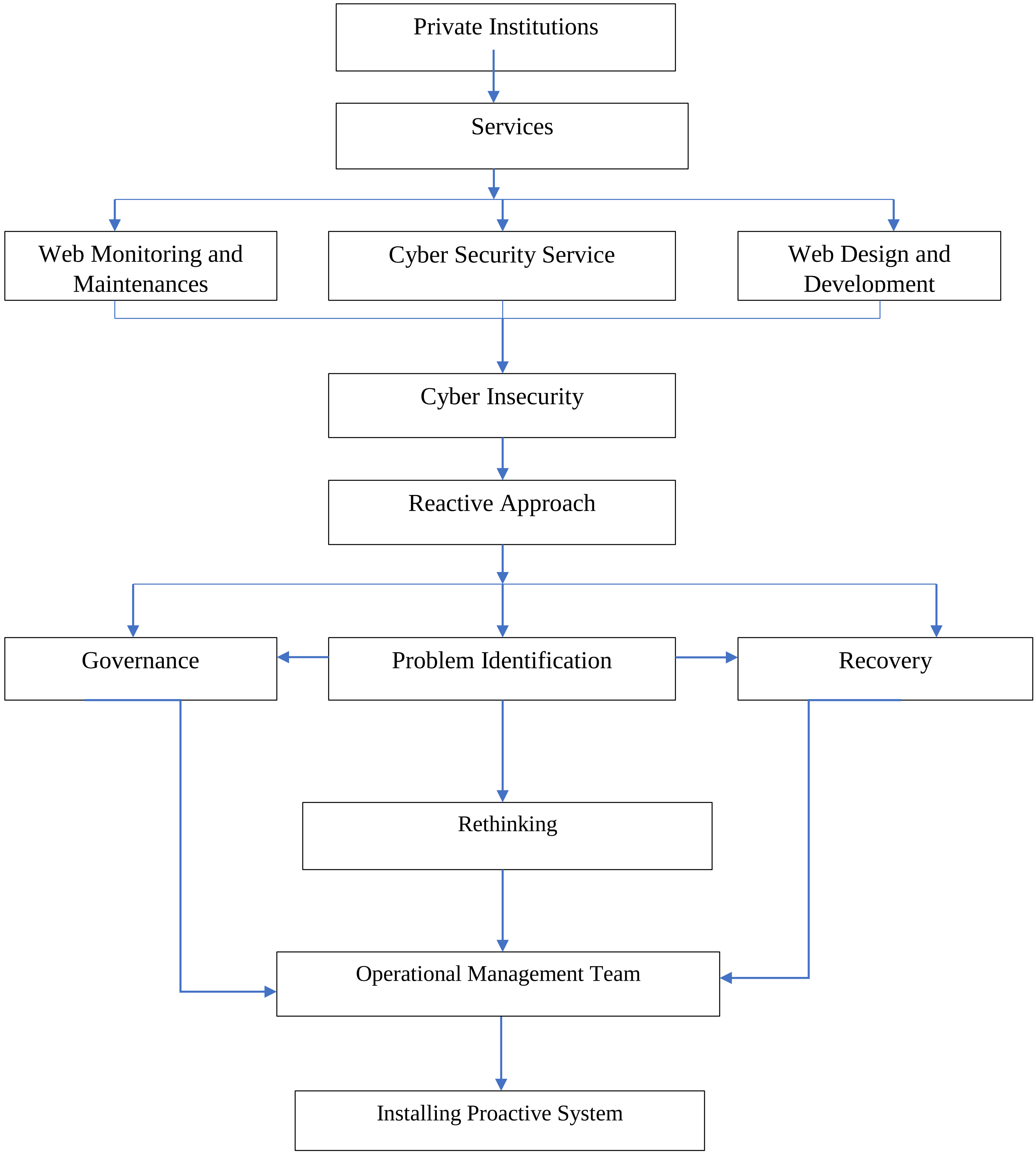

Figure 3.11: Conceptual Framework for Institutional Approach to Cyber Security.

7.4 Cyber Security Services:

From the perspective of private institution, the cyber security services have illustrated in two parts. Depending on the type of client and the nature of problems, private institutions were solving both individual and organizational cyber issues. 80% cyber institutions think that they are acknowledge about contemporary cyber risks and they did not require help from other institutions. It means, the strength of most institutions taken part on this study have confident to identify problems regarding organizational and individual cyber issues. But 20% institutions require jointly approach to deal with contemporary approach.

8. Conclusion

Cyber security can ensure safe browsing, internet base trading, communication. The trust of people and organizations on internet browsing is important. Increasing number of advance gear and software made our life easy but hidden insecurity lies on the overarching question that; The unauthorized access or monitoring on personal information or the threat of unethical use of the information. Private institutions are need to bring in the priority box considering the larger number of insecurity issues. Private cyber institutions need to consider as the IT resources of the country. Nowadays, Critical Information Infrastructural collapse is a prime concern for the organizations especially for financial sectors. The number of private institutions in Bangladesh is still unknown. There is no official number found for those institutions involve in baking security or dealing with organizations website monitoring. This study reveals that the business of Information Technology and Cyber Security services start with the conventional Trade License. Most the cases, the certification process remain unknown. But the contribution of private cyber institutions is spreading so fast. They need to bring under a regulative framework so that the entitlement of the business can be ensured and more IT experts get chance to bring their idea to build a safe information infrastructure.

9. Recommendation

Understanding a cyber-security problem is critical matter. It is tough job for any educational institution to prepare a top information security specialist which requires deep understanding of concepts from various information technology fields like system administration, networking, programming, databases, etc. (Furtuna et.al., 2010). On the other side, co-operative approaches among private institutions need to develop for a better security system. Private institutions should be more proactive. Private institutions are often neglected in policy planning. They need to include in the mainstreaming development agenda so that public-private partnership can be ensured. International and Regional partnership should also include so that transnational cybercrime can be prevented with joint operation. Furthermore, Department of ICT need to develop a guideline for the private cyber institutions. The guideline will ensure the legal access of IT professionals to deal with organizational cyber issue. Financial organizations those who allows internet base transaction need to develop a proactive approach so that unauthorized access can be prevented and critical information remain safe. As Private institutions are dealing with important and critical cyber issues of different public and private institutions, Government should consider their progress with high priority and scholarships. Ministry of ICT should arrange a training for the Private institution’s IT professionals especially those who deal with website management and cyber security issues. Knowledge areas of IT professional need to enrich with government policies and provisions. Especially, they need to have a clear understanding on *Digital Security Act-2018* so that a bridge can create between private cyber institutions and policy planners. To some extent advance training required for the private cyber professionals.

References

[1] Arquilla, J., and Ronefeldt, D. (1993). *The Advent of Netwar.* Santa Monica: RAND

[2] Arquilla, J., and Ronefeldt, D. Eds. (2001). *Networks and Netwars: The future of terror, crime and militancy*. Santa Monica: RAND.

[3] Btrc.gov.bd. (2019). Internet Subscribers in Bangladesh June, 2019. BTRC. [Online]. Available at: http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2019 [accessed 16 August 2019].

[4] Bendrath, R. (2003). The American Cyber-Angst and the Real World-Any Link? In. *Bomb and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham. New York: The New Press

[5] Cavelty, M.D. (2008). Cyber-terror-looming threat or phantom menace? The framing of the US cyber threat debate. *Journal of Information Technology and Politics*. Volume: 4, Issue: 1, pg. 19-36. DOI: 10.1300/J516v04n01_03. [Online].

[6] Der Derian, R.J. (1992). *Antidiplomacy: Spices, Terror, Speed, and War.* Oxford: Basil Blackwell.

[7] Der Derian, J. (2003). The Question of Information Technology in International Relations. *Millennium,* 32(3), 441-456.

[8] Deibert, R.J., AND Stein, J.G. (2002). Hacking networks of terror. *Dialog-IO*. Vol. 1. Issue 01, pp. 1-14.

[9] Link: http://dx.doi.org/10.1300/J516v04n01_03.

[10] Deibert, R.J. (2003). Black code: Censorship, Surveillance, and the Militarisation of Cyber-space. *Millennium*, 32(3), 501-530.

[11] Finn, P. (2007). Cyber Assaults on Estonia Typify a New Battle Tactic. *The Washington Post,* May 19.

[12] Furtuna, A., Patriciu, V.V, Bica, I. (2010). A structured approach for implementing cyber security exercises. *IEEE.* Pg. 415-418.

[13] Hansen, L., and Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly,*53, 1155-1175.

[14] Latham, R. (2003). Introduction. In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security,* edited by Robert Latham. New York: The New Press.

[15] Kamruzzaman, M., Islam, M.A., Islam, M.S., Hossain, M.S., and Hakim, M.A. (2016). Plight of youth perception on cyber-crime in South Asia*. American Journal of Information Science and Computer Engineering*, 2(4), 22-28. ISSN: 2381-7488.

[16] Kaspersky (2019). What is cyber security? [Online] Available at: https://www. Kaspersky.com/resource-centre/definitions/what is cyber security. [22 August, 2019].

[17] Sofear, A.D. & Goodman, S.D. (2000). *A proposal for an international convention on cyber-crime and terrorism*, Stanford, CA: Center for International Security and Cooperation, Stanford University..

[18] UNODC (2019). *Cybercrime Module 1 Introduction and Learning Outcomes*. [online]. Available at: http://www.unodc.org/e4j/en/cybercrime/module 1/ Intoduction-and-Learning Outcomes.html [Accessed 23rd Oct 2019]

[19] Weinman, G. (2004). www.terror.net. *How modern terrorist uses internet the Internet.*(United States Institute of Peace, Special Report 116), Washington DC: United States Institute of Peace.