‘Cyber Security’- A Concern for Improving Public Service Delivery: Challenges and Way Forward

Research Team

Mr. Md. Shaiful Islam, Joint Secretary, Cabinet Division

Mr. Mohammad Ashraful Alam, Deputy Secretary, Cabinet Division

Mr. Mohammad Wahiduzzaman Khan, Senior System Analyst, Cabinet Division

Cabinet Division

Government of the People’s Republic of Bangladesh

June 2023

‘Cyber Security’- A Concern for Improving Public Service Delivery: Challenges and Way Forward

Table of Contents

Acknowledgement

The research team would like to express their gratitude and appreciation to Mr. Md. Mahbub Hossain, the honorable Cabinet Secretary of the Government of Bangladesh, for providing the opportunity to conduct a study on 'Cyber Security'- A Concern for Improving Public Service Delivery: Challenges and Way Forward. The Team is grateful to Mr. Md. Mahmudul Hossain Khan, the esteemed Secretary (C&R) of the Cabinet Division, for his true direction and inspiration of the research.

In addition, Team is also grateful to the Research Management Committee of the Cabinet Division for their instructions and for facilitating the team with keeping the work in the right direction. We also acknowledge the support and cooperation of our colleagues at the Cabinet Division throughout the research endeavor.

Again, the team expresses regards and thankfulness to the officials of ICT Division and subordinate offices for their cooperation in providing necessary information during data collection phase. We are also indebted to the experts of a2i, BGD -e-GOV-CIRT and IT experts of Bangladesh Bank who provided valuable opinion on the issue.

Moreover, Team thanks to the all respondents of the study in providing their feedback and opinion through questionnaire and FGD with an aim to make the study effective.

Finally, Team would like to convey gratefulness to the family members for their continuous support and encouragement.

Study Team

Abbreviation

BASIS	Bangladesh Association of Software & Information Services
BDCCL	Bangladesh Data Centre Company Limited
BIID	Bangladesh Institute of ICT in development
BIGM	Bangladesh Institute of Bank Management
BNDA	Bangladesh National Digital Architecture
BTCL	Bangladesh telecommunication Company Limited
BTRC	Bangladesh Telecommunication Regulation Commission
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, and Availability
CIRT	Computer Incident Response Team
CSIS	Centre for Strategic & International Studies
DDOS	Distributed Denial of Service
DOS	Denial of Service
DU	University of Dhaka
EFT	Electronic File Transfer
FGD	Focus Group Discussion
GOBISM	Government of Bangladesh Information Security Manual
ICT	Information & Communication Technology
IDS	Intrusion Detection System
ITU	International Telecommunication Union
LAN	Local Area Network
NIST	National Institute of standard & Technology
NPM	New Public Management
NSDA	National Digital Security Agency
SSRF	Server Side Remote Request Forgery
UIA	United American University
UNDP	United Nations Development Program
UNESCAP	United Nations Economic & Social Commission for Asia & The Pacific

Abstract

Cyber security is crucial for the continuous growth and development of Bangladesh's digital economy and the protection of its citizens and critical infrastructure. The advancement in technology has led to increased use of electronic platforms in service delivery in all sectors including public administration creates an extra focus on cyber security concerns in e-governance. The online service activities have brought the risks of cyber security breaches, which can compromise sensitive information and undermine public trust in e-governance. Though measures have been taken regarding cyber security issues in Government Offices, still there are gaps.

The primary objective of the study was to examine the challenges of cyber security to service delivery in the public Administration. Data have been collected using questionnaire survey of 106 respondents from government offices and also three Focus Group Discussion (FGD) have been conducted. Data analysis revealed that there exist cyber security threats & vulnerabilities regarding digital public service delivery. This study identified the cyber security issues i.e. present status, cyber threats, vulnerabilities, awareness among employees, steps taken to ensure cyber security in the offices of Public Administration in Bangladesh.

The findings suggests that government officials should be aware & sincere to mitigate cyber threat. Public office shall use license version & update software and shall avoid to use pirated software. Regular internal & external IT audit should be performed. There is great shortage of skills cyber professional personal. So adequate training is necessary. The study also recommends to appoint a dedicated cybersecurity officer to oversee the implementation of cybersecurity & reduce vendor dependency; to comply strict password policy & two factor authentication/ multi factor authentication policy in public office and also need to proper monitoring & continuous collaboration, cooperation and threat information sharing among government entities to combat cyber threat.

Keywords:

Public Service, Cyber Security, Information Security, Cyber Threat, Cyber Vulnerability, Authentication.

‘Cyber Security’- A Concern for Improving Public Service Delivery: Challenges and Way Forward

Chapter-1

1.0 Background of Study

Cybersecurity is becoming increasingly important in Bangladesh as the country becomes more digitized and connected to the internet. Increased IT infrastructure has given rise to enormous chances of security breach. Digitization is happening in Bangladesh for last few years at an appreciable rate (UNDP, 2021). With the growing number of internet users and the increasing use of online platforms for service delivery and other activities, the risk of cyber threats has also increased. Cybersecurity is crucial for the continued growth and development of Bangladesh's digital economy and the protection of its citizens and critical infrastructure.

The government of Bangladesh has launched extensive development initiatives to make Bangladesh a developed nation by 2041 (Vision 2041). The government has also declared Bangladesh as smart Bangladesh and it has drafted strategy on smart Bangladesh master plan 2041 (SMART Bangladesh, 2023). It aims to be at the forefront of achieving Honorable Prime Minister Sheikh Hasina’s vision of transforming Bangladesh to a smart Bangladesh by 2041, where there are four pillars of smart Bangladesh as smart government, smart citizens, smart society and smart economy (SMART Bangladesh, 2023). The Digital Bangladesh program was launched in 2009. In order to implement Digital Bangladesh, all government ministries, departments, directorates, organizations, and institutions are now engaged in a variety of initiatives (Digital information security guideline- 2017). As a part of this program, a significant number digital services and platforms have been launched on line with its vision of transforming the country into digital Bangladesh [3]. Some of these are- National web portal, National Data Transmission, Birth and Death Registration, National Identity Card, e-Land Information and Service Framework, e-Documents, e-Nothi, e-Procurement, e-Banking, EFT, e-Tax, e-Ticketing, National e-Database, e –chest, e-mutation etc (Aspire to Innovate, 2022). This ever-increasing digitalization is leading to create huge information about service delivery in public administrations to offer customer-friendly services to citizens and businesses.

As Bangladesh undergoes rapid socio-economic transformation with its GDP growing more than 6% per annum over the last decade, substantial challenges remain in building Digital/Smart Bangladesh which aims to accelerate country's transformation using the ICTs. The public sector is increasingly using ICT in delivering services and as result most of the public offices are utilizing internet. At present, more than 52,000+ government department websites have been developed in the 'Bangladesh National web portal. Total number of offices using E-nothi (including all Ministries/Departments and Departmental Organizations) as on June 2022 is 11,308. Out of 2,425 public services in government offices, 1,851 services have been digitized. More than 8,800 Union Digital Centers have been launched in the country to facilitate access to public services for underserved citizens (Aspire to Innovate, 2022). So, every government office has come under the connection of internet and huge volume of information is exchanging regularly among service receiver and government offices. Moreover, every public officer is paid to have internet connection and also paid by the government for using mobile phone. Therefore, most of the public employees use internet for delivering public service.

Again, Bangladesh has one of the fastest growing internet users in the world. The number of internet users is increasing day by day very rapidly. The mobile operators and internet service providers are also working on making the internet available to all the users at an affordable condition. The universities are equipped with Wireless internet throughout the campus. Even public places are offering Wi-Fi hotspots. All the factors have facilitated towards the number of increased internet users in our country. A study shows that till December 2018 almost 91 million people of Bangladesh are internet subscribers. Among them, 86 million are mobile internet users [Chowdhury, A., and H. Zaman, 2014]. So, it is very much imaginable, mobile internet has created a boom in online service usage. According to Wikipedia, there are almost 90 million smartphone users in Bangladesh. This smartphone consumes a huge amount of data and people are constantly using a lot of services like photo sharing, social networking, file sharing etc. Mobile banking has also become very common. Banks are also providing their services over the internet to their customers through mobile applications. People are using ride-sharing application, online shopping etc. and all other types of activities.

In the modern world, the internet is an open source of knowledge for everyone. Information is now easily accessible and reasonably priced thanks to the Internet, Local Area Network (LAN), and other technologies including computers, servers, laptops, mobile phones, social media, wireless, television, etc. Events and logs are generated by using internet activities

(Haque, 2019). These occurrences are creating data. Users' identities and signatures are becoming publicly available due to online activity. The task that we are doing, the file that we are sharing as long as it is over the internet they can be breached. If there is a big data breach caused by a lack of cyber security infrastructure, the results might be disastrous (Haque, 2019). As a result, suitable security measures must be taken when using and storing information. Cyber-attacks are becoming a hindrance to the appropriate handling and use of digital information. Numerous organizations are dealing with cyber-attacks such as data breaches, data theft, distributed denial of service etc. due to a lack of information security capabilities, inadequate and poorly maintained security policies, specialized expertise, and qualified people. To safeguard digital information resources from all of these attacks, sufficient administrative security measures need to be taken.

In recent years, this increasing use of technology in public administration has led to an increased focus on cyber security concerns in e-governance. E-governance refers to the use of digital technology to enhance the efficiency and effectiveness of public administration. The use of technology in e-governance has the potential to improve service delivery, reduce costs, and increase transparency. However, with the benefits of technology come the risks of cyber security breaches, which can compromise sensitive information and undermine public trust in e-governance.

1.1 Public Administration, Public Services & E-Governance:

Public administration is responsible for all public services. Since the 19th century, academics, practitioners, and researchers of public administration have been looking for a viable paradigm for successful and efficient public administration. Based on the surrounding circumstances, the paradigm modifies to reflect reality. In the context of the global ICT revolution, the evolution of e-governance follows the paradigm change in public administration.

In his article "The Study of Administration", Woodrow Wilson (1887), emphasized on the concerns of public administration as: what the government can accomplish effectively and correctly and how it may carry out these right actions with the greatest possible efficiency and at the lowest possible expense, either in terms of money or energy. The principles of public administration and the objectives of providing public services are laid forth in Woodrow Wilson's notion of public administration.

The bureaucratic model of Max Weber (1947) aims to improve the efficiency of public organizations, is characterized by task specialization, written rules and procedures, a structure of authority, rationality, merit-based hiring, and impersonality. Because of its strict adherence to rules and regulations, wasteful use of resources, and unproductive use of resources, Weber's bureaucracy was unsuccessful (UN 2003). According to Zafarullah and Siddiquee (2001), the public sector is plagued with inefficient service delivery, bribery, irresponsible behavior on the part of officials, bureaucratic favoritism, and clientelism. In contrast, the private sector's management strategy was successful and efficient, which put pressure on the bureaucracy. These limitations and presumptions led to the emergence of the New Public Management (NPM) paradigm of public administration, which gradually transformed public administration into public management.

Government officials are pushed to adopt new governance models as government operations become increasingly complex. Governmental systems with a traditional hierarchical structure have lost their effectiveness. It was impossible to resolve problems with strict bureaucratic procedures. Developing countries like Bangladesh also had trouble implementing NPM. Thus, towards the start of the 1990s, the World Bank, UNDP, and other international agencies pushed the concept of good governance. Public institutions must successfully manage public resources and carry out public business in order to exercise good governance. According to the UNESCAP (2009), good governance is defined as being fair and upholding the rule of law, as well as democratic, consensus-oriented, accountable, open, adaptive, and efficient.

E-government is regarded as a key paradigm for bringing openness and making the public sector efficient, effective, and responsive to citizens in order to actualize the ideas of good governance. E-Governance, according to the World Bank (2014), is the use of ICT by governmental entities to change how they interact with the public, private sector, and other parts of the government. The reform and modernization of the public sector might greatly benefit from the use of ICT in the form of E- Governance (Naz, 2009). Using information and communication technology (ICT), the E-Government framework enables public sector entities to perform effective services at the local and national levels. Bringing government closer to the people is one of the main goals of e-government. Governments all over the world have acknowledged that ICT is one of the critical elements required for effective public sector reform, even if it has been the driving force behind E-government initiatives (Maio 2006). E-Government is therefore viewed as a crucial instrument for achieving good governance and enhancing the provision of public services.

1.2 Information Security, Internet Security & Cyber Security

Information Security, Internet Security & Cyber Security are critical concepts that are all related to protecting digital information from unauthorized access, theft, and damage. Information security refers to the process of safeguarding information by implementing various measures to prevent unauthorized access, disclosure, or modification of data. It involves protecting both digital and physical information, including data on computers, servers, mobile devices, and other storage media. Information security is basically comprised of ensuring five key terms – confidentiality, integrity, network security, application security, and host security (Usher A., 2006). The NIST (2018) states that information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

There are three protection goals in information security: confidentiality, integrity and availability (Anderson 1972; Voydock and Kent 1983), commonly referred to as the 'CIA triad'.

Security Triad (CIA).

Security measures have the purpose of addressing one or more of these objectives, as follows: – Confidentiality: prevent unauthorized information gain; Integrity: prevent or detect unauthorized modification of data; & Availability: prevent unauthorized deletion or disruption.

"Internet" is defined by Section 2(8) of The Information & Communication Technology Act, 2006 as an international computer network by which users of computer, cellular phone or any other electronic system around the globe can communicate with one another and interchange information and can browse the information presented in the websites. Internet security is the practice of ensuring that the internet and its connected systems, including websites, networks, and applications, are secure and protected from cyber threats such as viruses, malware, and hacking attempts.

On the other hand, Cyber security is a broader term that refers to the protection of all forms of digital assets, including computers, networks, servers, mobile devices, and other electronic

systems, from cyber-attacks. Cyber security is the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets (ITU, 2014). So, it encompasses two terms- Information Security that includes preservation of confidentiality, integrity and availability of information and Network Security which includes protection of networks and their services from unauthorized modification, destruction or disclosure and provision of assurance.

Effective Information Security, Internet Security & Cyber Security measures are critical for individuals, businesses, and governments to protect sensitive information and prevent potential damage and financial losses resulting from cyber attacks. Such measures may include implementing firewalls, using secure passwords and authentication systems, regularly updating software and systems, and providing training to employees and users to prevent phishing and other cyber attacks.

1.3 Cyber-Threat & Cyber Attack, Cyber Vulnerability, Cyber Risk, Cyber Crime & Cyber Space

1.3.1 Cyber threats & Attack

Threat is an object, person or other entity that represents a constant danger to an asset (Whitman & Mattord, 2008). It is anything that can exploit vulnerability, intentionally or accidentally and damage or destroy an asset. Cyber threats refer to various malicious activities that target computer systems, networks, and digital devices, including unauthorized access, data theft, phishing attacks, malware infections, ransomware, and more. These threats can cause significant harm to individuals, businesses, and government organizations. A cyber threat is a potential danger or risk that can cause harm to a computer system or network. Cyber threats can come in different forms, including malware, viruses, spyware, and phishing attacks etc. Cyber threats can also be caused by insider threats or unintentional human error.

On the other hand, A cyber-attack is a deliberate and malicious attempt by hackers to breach a computer system or network with the intention of stealing data, disrupting operations, or causing damage. Cyber-attack can be carried out through various means such as malware, phishing, social engineering, or exploiting vulnerabilities in software or hardware. Examples

of cyber attacks include ransomware, denial-of-service (DoS) attacks, and man-in-the-middle attacks (Tushar P. Parikh et al. 2017)

One example of a cyber-attack is the WannaCry ransomware attack (2017) affected more than 200,000 computers in 150 countries, encrypting users' data and demanding payment in Bitcoin for its release. It was estimated to have caused billions of dollars in damages. The ransomware was able to spread quickly through a vulnerability in the Windows operating system, which had been exploited by the attackers. The attackers demanded ransom payments in Bitcoin in exchange for decryption keys to unlock the encrypted files.

Cyber-attacks are currently emerging as a barrier to proper storage and use of digital information. Due to lack of information security capabilities, weak and mismanaged security controls, lack of specialized knowledge and skilled manpower, various organizations are facing cyber-attacks through data breaches, data theft, distributed denial of service etc. It is necessary to take adequate administrative security measures to protect digitized information resources from all these attacks.

1.3.2 Cyberspace

Cyberspace is the realm of computer networks (and the users behind them) in which information stored, shared, and communicated outline (Singer and Friedman, 2014). Cyber space Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval and exploitation of information (Ahmed Jamal et al., 2021; Alghamdie, 2021; Bullock et al., 2021; Ashraf et al., 2021). Secure cyberspace is a key element of protecting national security is the age of globalization.

1.3.3 Cybercrime

Cybercrime is referred to as any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them (Ayofe & Irwin 2010). Cybercrime refers to criminal activities that are committed using the internet, computer systems, or other forms of digital technology. These activities can range from hacking and identity theft to cyberbullying and the distribution of illegal content. Cybercrime is a growing concern worldwide, as the proliferation of technology has made it easier for criminals to carry out illegal activities online. According to the United Nations Office on Drugs

and Crime (UNODC), cybercrime can be defined as "an unlawful act or series of acts committed using a computer system or network, either as a target or a tool, to perpetrate criminal or fraudulent activities." (UNODC, 2013). According to the U.S. Department of Justice (2020), cybercrime "encompasses any criminal activity that involves a computer, networked device, or a network".

1.3.4 Hackers

Hackers: A hacker is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means. There three types of hackers:

Black Hat Hacker: Black-hat Hackers are also known as an Unethical Hacker or a Security Cracker. These people hack the system illegally to steal money or to achieve their own illegal goals. Black hat hacking is illegal.

White Hat Hacker: White hat Hackers are also known as Ethical Hackers or a Penetration Tester. They hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray hat Hackers: Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

1.3.5 Cyber Risk

Risk is the potential loss, damage or destruction of an asset as a result of a threat exploiting vulnerability. A risk is a possibility that something unpleasant will happen. According to the NIST, (2018), cyber risk is "the potential adverse effects on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or society that may result from the exploitation of vulnerabilities associated with the use of information technology. Cyber risks can include unauthorized access to sensitive information, system downtime, theft or destruction of data, and reputational damage. These risks can arise from a variety of sources, including external hackers, insider threats, or unintentional errors. Organizations must manage cyber risk through

effective security policies, procedures, and technologies. This includes identifying and prioritizing assets that are most critical to the organization's operations, implementing appropriate safeguards, and regularly assessing and updating the organization's risk management strategy.

1.3.6 Cyber Vulnerabilities

Cyber vulnerabilities refer to weaknesses or flaws in a computer system, software\ or network that can be exploited by malicious actors to compromise the security and integrity of the system. These vulnerabilities can be present in various components of a system, such as hardware, software, and human factors. According to the NIST, (2020), "A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source".

Common examples of cyber vulnerabilities include outdated software, weak passwords, unpatched systems, and misconfigured network devices. Exploiting these vulnerabilities can result in various cyber-attacks, such as malware infections, data breaches, and denial-of-service attack.

One example of a cyber vulnerability is the Heartbleed bug, which affected OpenSSL, a widely used cryptographic library. The bug allowed attackers to read sensitive information, such as passwords and private keys, from the memory of affected systems without leaving any trace. The Heartbleed vulnerability was discovered in 2014 and affected an estimated 17% of all secure web servers at the time (OWASP, 2017).

1.4 Present Scenario of Cyber Security in Bangladesh

Bangladesh has been facing an increasing number of cyber threats in recent years. Public service delivery, such as e-governance, banking services, and healthcare services, has also become a target of cybercriminals. In Bangladesh, Cybercrimes are divided into two broad categories on the basis of its nature - direct and indirect (Nur Nabi & Tanjimul, 2014). Direct cybercrimes are such as malicious mail, pornography, use of e-mail for illegal activities, use of internet for transmitting false and malicious information, use of internet for prostitution, use of internet for women and child trafficking etc. On the other hand, indirect cybercrimes are like pathways for traditional crimes such as kidnapping, robbing banks, committing murders, threatening and demanding money by using exclusive pornographic videos and pictures (photo-shopped in most cases) etc. (Nur Nabi & Tanjimul, 2014). BGD e-GOV CIRT has identified

some cyber threats in Bangladesh which have occurred in 2021, these are ransomware, malware, phishing, spam, insider threats, web based attack, denial of services, data breach, espionage, etc. and at the same time BGD e-GOV CIRT also identified some cyber vulnerabilities in Bangladesh like Apache foundation log4j library, server side remote request forgery (SSRF), windows print spooler remote code execution, microsoft office memory corruption vulnerability, blue keep vulnerability etc. (Landscape, 2021).

Bangladesh's Computer Incident Response Team (CIRT) (BD cyber Landscape, 2020) reported a significant increase in cyberattacks, with a total of 17,334 incidents reported, including malware, phishing attacks, and DDoS attacks. In addition, several high-profile cyberattacks have occurred, such as the hacking of the Bangladesh Bank in 2016, where hackers stole $81 million. According to a report by Bangladesh Association of Software and Information Services (BASIS) in 2021, the country witnessed a significant rise in cybersecurity incidents during the COVID-19 pandemic. The report shows that the number of cyber-attacks in Bangladesh increased by 650% in 2020 compared to the previous year. In another report published by Bangladesh Telecommunication Regulatory Commission (BTRC) in 2020, it was found that phishing attacks, identity theft, and data breaches were the most common types of cyber-attacks in the country. The report also revealed that the banking and financial sector was the most targeted industry.

Moreover, a study conducted by the Center for Global Communication Studies at the University of Pennsylvania found that political parties and journalists in Bangladesh were vulnerable to cyber-attacks. The study suggests that political parties were targeted by hackers to steal confidential data, while journalists were targeted to silence their critical voices. A study conducted by Bangladesh Association of Software and Information Services (BASIS) in 2020 reported that around 60% of the country's businesses had suffered some form of cyber-attack in the past year. The most common types of attacks included phishing, malware, ransomware, and social engineering. In December 2020, the Bangladesh Telecommunication Regulatory Commission (BTRC) reported that the country had experienced over 10,000 cyber-attacks in just six months. The majority of the attacks were aimed at disrupting the country's financial sector and government institutions.

The financial sector has been a prime target for cyber-attacks in Bangladesh. In 2019, five major banks in the country were hit by a cyber-attack that resulted in the theft of millions of dollars. The attack was carried out using malware that was able to bypass the banks' security

systems. The healthcare sector has also been hit hard by cyber-attacks in Bangladesh. In 2020, the country's largest hospital, Dhaka Medical College Hospital, suffered a ransomware attack that resulted in the loss of patient data.

The government of Bangladesh has taken several measures to improve cybersecurity in the public service delivery arena, such as establishing the Bangladesh Telecommunication Regulatory Commission (BTRC) to regulate and monitor the country's telecommunications sector, and the Bangladesh Computer Council to oversee and coordinate the country's IT sector. The government has also introduced the Digital Security Act to address cybercrimes and protect citizens' online rights. The government has also established a Computer Emergency Response Team (CERT) and a National Digital Security Agency (NDSA) to address cybersecurity threats. Additionally, the government has passed the Digital Security Act in 2018 to regulate online activities and prevent cybercrime.

Bangladesh has secured the top position among the South Asian countries in the National Cyber Security Index (NCSI) prepared by Estonia-based e-Governance Academy Foundation (DHAKA, Aug 24, 2021 (BSS). NCSI was established to evaluate basic cyber-attack preparedness, cyber events, criminal activity, and major crisis management efforts. Bangladesh ranking in 53rd place 2021 with a score of 81.27. Last year, Bangladesh was ranked 78th in the index, Global Cyber Security Index-2020 (ITU- International Telecommunication Union (ITU)

However, there is still much to be done to improve cybersecurity in Bangladesh. Some of the challenges include inadequate infrastructure, lack of skilled cybersecurity professionals, and low cybersecurity awareness among the public. Additionally, the COVID-19 pandemic has increased the demand for digital services, leading to a surge in cyberattacks. Overall, cybersecurity in the public service delivery arena in Bangladesh is an ongoing concern that requires continuous efforts from the government and the private sector to address the evolving cyber threats.

1.5 Problem Statement

Cybersecurity is becoming increasingly important in Bangladesh as the country continues to develop its digital infrastructure; public services are delivering through e-service management and more people use smart devices for communication, commerce & other activities over the internet. These digital infrastructures, devices, e-services have their own

vulnerability issues as well as the data shared over the internet has very good chances of getting cyber-attack. Statistics shows that till now more than 4550 + incidents have been recorded by BD e CIRT and more than 278 government organizations have been come under attack (The Daly Star, 2022). As the number of internet user increases, the threats towards the cyberspace increases with it. According to the security report of Kaspersky in 2015, it is seen that Bangladesh places second among all the other countries in the field of malicious infection. The number of unique users who are prone to cyber-attack is 69.55%. For the most part, these attacks are spam attacks. Almost 80% of them are spam attacks says Trend Micro Global Spam map. Moreover, a recent study by Bangladesh Computer Council showed that a huge number of unique IP addresses which were infected belong to the popular mobile network operators. The number of IP address is approximately 34552 (The Daly Star, 2022).

Almost 1400 IP addresses have been used by hackers of Russia and Ukraine to launch cyber-attacks on each other. This revelation comes after a recent investigation conducted by BD e CIRT (Landscape, 2021). A high risk of cyber-attacks looms large over 36% of banks in Bangladesh mainly due to a shortage of investment in strengthening security measures, skilled personnel and a lack of awareness among bankers and customers. In addition, another 16 per cent of banks are in a very high-risk condition, an indication of the fragile cybersecurity scenario in Bangladesh's banking sector, according to research carried out by the Bangladesh Institute of Bank Management (BIBM) (Alam et al., 2023).

Considering the above scenario, it is obvious that there exists a high risk of cyber threats which is a challenge for delivering digital public service. There is also lack of proper awareness regarding cyber security issues among the public administration personnel and bodies which becomes a barrier to convert this country into a digital country. The present study will be able to identify the cyber security threats & vulnerabilities regarding digital public service delivery, measurement taken by public administration and also able to identify the cyber threats. This study will also propose some recommendation on cyber security issues.

1.6 Research Question

1. What is present status of cyber security in public administration of Bangladesh?
2. What are the cyber security threats for improving public service delivery?
3. What are the vulnerabilities in relating to cyber security for improving public service delivery?
4. What measures should be taken in public administration to address the cyber security challenges?

1.7 Objective

1. To know the present status of cyber security in public administration of Bangladesh;
2. To identify the cyber security threats for improving public service delivery;
3. To identify the cyber security vulnerabilities for improving public service delivery;
4. To make recommendations in relating to the cyber security.

1.8 Significance of the Study

The study will encourage govt. employees to develop suitable security measures and guidelines. This will also guide them when reviewing the current IT policies to improve cyber security in the public service delivery sector. The study will further aid IT officials to better understand and manage the cyber security risks facing the public service. Again, this study will help disseminating knowledge of cyber security among the employees to take measures of data center risk analysis & protection in protecting public service related information.

Chapter-2

2.0 Literature Review

The advancement in technology has led to increased use of electronic platforms in public service delivery. However, this has also brought about new challenges in the field of cybersecurity. it is discussed above that Cyber security encompasses both information and internet security and also refers to the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from digital attacks, theft, damage or unauthorized access. Cybersecurity challenges have become a significant problem for organizations, and the public sector is no exception.

Cybersecurity threats come in various forms, including malware, phishing, hacking, denial of service, and ransomware attacks etc. These attacks can have devastating consequences, including financial losses, loss of personal information, reputational damage, and legal liabilities. Thus, managers

need to know threats that influence their assets and identify their impact to determine what they need to do to prevent attacks by selecting appropriate countermeasures (Mouna Jouini et al. 2014).

Vulnerabilities consist of weaknesses in a system which can be exploited by the attackers that may lead to dangerous impact. When vulnerabilities exist in a system, a threat may be manifested via a threat agent using a particular penetration technique to cause undesired effects (Mouna Jouini et al. 2014). The financial threat loss to organizations could be significant. According to the 11th Annual Computer Crime and Security Survey 74.3% of the total losses are caused by: viruses, unauthorized access, laptop or mobile hardware theft and theft of proprietary information (Mouna Jouini et al. 2014).

Mouna Jouini et al. (2014). identified threats in two ways: techniques that attackers use to exploit the vulnerabilities in the system components or impact of threats to assets. they have proposed a model known as the multi-dimension's threats classification model. in their model they placed in different types of security threats in to five classes- 1. viruses and computer worms are threats caused by intentional, malicious, insider's human actions that can cause high level of information and resources destruction.; 2. Terrorism and political warfare are caused by intentional, malicious, outsider's human actions; 3. Passwords change, failing to log off before leaving a workstation, careless discarding of sensitive information are malicious accidental insider human actions ; 4. Sabotage, data theft, data destruction and spoofing attacks are threats caused by human outsider intentional agents. They caused malicious damage like the corruption of data; 5. Wildfire, flooding, earthquakes and tidal waves are caused by accidental external natural phenomena and allow serious impacts like destruction end corruption of data and resources.

Microsoft developed a classification method, called STRIDE, which characterize the threats as Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service and Elevation of privilege (Meier et al., 2003).

The ISO standard (ISO 7498-2) has listed five major security threats impacts and services as a reference model: Destruction of information and/or other resources, corruption or modification of information, theft, removal or loss of information and/or other resources, disclosure of information, and interruption of services.

An Empirical Study by Shweta Mittal & P. Vigneswara Ilavarasan identified some factors of cyber security i.e. leaving printouts, links from known source, website access, information in website, password complexity, plugging USB in public places.

Farahmand et al. (2005) in their study surveyed 280 potential respondents to assess the implementation of cybersecurity practices such as cyber policy, risk management, and training and awareness. According to the survey, most government entities have very little or no implementation of

cybersecurity policies, risk management, awareness, and incident management. It also suggests that a large number of organizations have experienced cybersecurity risks including hacking, malware, and phishing scams, or have been negatively impacted by them.

Usmani K. (2008) identifies the threats to information security in four broad categories: malware, attack through e-mail, spam associated threats, and phishing. These categories of security threat is causing hacking of credit card information, system information, and account information, stolen user ID and passwords, unauthorized access to confidential information, Loss of intellectual property, remote access of PC, and theft of customer data, dangerous viruses, worms, trojans, and spywar.

Usmani K. (2008) also suggested a must use of updated antivirus, anti Spyware, and spam filters to avid phishing. To ensure highest level of information security, the State Bank of India manages their information security based on six pillars – security governance, consulting, compliance, incident control, monitoring, and security awareness for its stakeholders (Kishore. P., 2008).

Usher A. (2006) mentioned in his study some traditional threats like hacker activity, worms & viruses, spam, spyware, and phishing and also suggested five points for protection from the threats - assessing technology environment regularly, adapting updated security policy, having a rigorous and effective user awareness plan, putting policies and procedures into action effectively, and finally assess effectiveness and revising policies if needed.

Bangladesh has experienced a surge in cybercrimes in recent years. According to a report by the Bangladesh Association of Software and Information Services (BASIS), the country saw a 350% increase in cybercrimes between 2014 and 2017 (Ahmed, 2018). The report also found that the majority of these cybercrimes were committed through social media platforms and messaging apps such as Facebook, WhatsApp, and Viber. Some of the most common cybercrimes in Bangladesh include identity theft, phishing, hacking, and ransomware attacks.

One of the main challenges of cybersecurity in e-governance is the increasing sophistication of cyber attacks. According to a report by the World Economic Forum, cyber attacks are among the top five risks to global stability, with the potential to cause significant damage to public institutions and infrastructure (World Economic Forum, 2019).

Another challenge is the lack of awareness and preparedness among public officials and administrators. Many government agencies lack adequate cybersecurity measures, and often do not prioritize cybersecurity until an attack occurs (Chen, 2020). Additionally, there is a shortage of skilled cybersecurity professionals in the public sector, which makes it difficult to implement effective cybersecurity measures (Kshetri, 2017).

One of the main challenges in Bangladesh is the lack of awareness about cybersecurity among the general population. Many people in the country are not familiar with the risks of using the Internet and do not take the necessary precautions to protect themselves. For example, a survey conducted by the Bangladesh Telecommunication Regulatory Commission (BTRC) found that only 7% of Internet users in the country use antivirus software (Zaman, 2017). This lack of awareness makes it easier for cybercriminals to carry out their activities.

Another challenge in Bangladesh is the lack of cybersecurity professionals. According to a report by the Bangladesh Institute of ICT in Development (BIID), there are only around 200 cybersecurity experts in the country, which is not sufficient to address the growing cybersecurity threats (Rahman, 2019). The shortage of cybersecurity professionals is a significant obstacle in developing effective cybersecurity policies and practices. According to a study by Frost & Sullivan (2020), there will be a shortage of 1.8 million cybersecurity professionals by 2022. This shortage can lead to increased vulnerability to cyber-attacks and difficulty in responding to them. To address this challenge, organizations can invest in training and education programs to develop the necessary skills among their employees.

One of the studies conducted by Symantec (2020) identified that phishing attacks were the most common type of cybercrime in 2019, accounting for 25% of all reported incidents. The study also revealed that ransomware attacks had increased by 18% in 2019 compared to 2018, with small and medium-sized businesses being the most targeted. Similarly, Ponemon Institute (2020) reported that data breaches caused by cyberattacks had increased by 17% in 2019, with the healthcare and financial sectors being the most targeted.

A study conducted by the Center for Strategic and International Studies (CSIS) (2019) revealed that the most significant cyber threats facing organizations included phishing attacks, ransomware, and advanced persistent threats (APTs). Similarly, a study conducted by Accenture (2020) identified that insider threats were the most significant cyber threat facing organizations, accounting for 60% of all cyber incidents.

One of the major challenges facing e-governance in relation to cyber security is the lack of awareness and training among government officials and employees. This is highlighted in a study by Sabherwal and Chan (2001), which found that many government employees lacked the necessary knowledge and skills to use technology securely. This lack of awareness can lead to unintentional security breaches, such as the use of weak passwords or the sharing of sensitive information.

Md. Sadek Ferdous, (2020) have shown in their study that password is a strong cyber security factors in Bangladesh. Muhammad Saifuddin Khan & Suborna Barua (2009) in their study found challenges that Lack of adequate knowledge , Lack of Proper Training , Do not have quick response ability , Lack of Active Government Responses to the need , Not Updated with the high end solutions regularly (time lag exists) and Human Resource Constraint.

Another challenge is the rapid pace of technological change, which can make it difficult for governments to keep up with the latest cyber security threats and solutions. This is discussed in a report by the World Bank (2012), which argues that governments need to invest in research and development to stay ahead of cyber criminals.

.One of the main challenges of cybersecurity in e-governance is the complexity of government IT systems. Public administration systems often involve multiple departments, agencies, and levels of government, which can make it difficult to ensure consistent and comprehensive cybersecurity measures across the entire system (Mbarika et al., 2020). Another challenge is the lack of cybersecurity expertise and resources in the public sector, which can lead to inadequate risk assessment and mitigation strategies (Lambrinoudakis et al., 2020).

Several studies have highlighted the importance of developing a comprehensive cybersecurity framework for e-governance. For example, Lee et al. (2020) proposed a risk-based framework that considers the unique characteristics of government systems and provides a systematic approach to identify and mitigate cybersecurity risks. Similarly, Bhatia and Jha (2021) suggested a cybersecurity maturity model that can help governments assess their cybersecurity posture and develop strategies for improvement.

Ahmed, M., & Hasan, M. R. (2019). This study provides a comprehensive review of the cybersecurity vulnerabilities in Bangladesh, including social engineering, malware, ransomware, phishing, and other cyber threats. The authors highlight the need for effective cybersecurity policies and strategies to address these vulnerabilities.

Islam, M. A., & Abdullah, M. S. (2019) provide an analysis of the current cybersecurity status in Bangladesh and identifies the future challenges that the country may face in terms of cybercrime. The authors discuss the need for a comprehensive cybersecurity strategy that addresses both technical and non-technical aspects of cybersecurity.

Hossain, M. S., & Rahman, M. R. (2020). This study reviews the existing literature on cybersecurity vulnerabilities and threats in Bangladesh, including cybercrime, cyber espionage,

and cyber terrorism. The authors identify the need for a multi-dimensional approach to cybersecurity that includes technical, legal, and socio-economic aspects.

Uddin, M. A., & Islam, M. S. (2019). Cybersecurity Challenges and Prospects in Bangladesh: A Review. International Journal of Computer Applications, 182(19), 12-17 This article provides an overview of the cybersecurity challenges and prospects in Bangladesh, including the lack of cybersecurity awareness, inadequate cybersecurity infrastructure, and insufficient legal frameworks. The authors suggest that a collaborative approach between the government, academia, and industry is required to address these challenges.

Karim, M. A., & Hasan, R. (2020) in their study explores the cyber security challenges in Bangladesh by conducting interviews with experts from various sectors. The authors identify the lack of awareness, insufficient funding, and inadequate legal frameworks as the major challenges faced by the country. They also suggest that the government should take a more proactive role in addressing these challenges.

Abouzakhar, et al. (2017) examine the cybersecurity vulnerabilities and threats in the healthcare sector. They identified various vulnerabilities, including weak passwords, unsecured networks, and outdated software. The authors argue that these vulnerabilities can lead to data breaches, which can compromise patient data and even result in identity theft.

Cyber Security Vulnerabilities in the Financial Sector" by A. Al-Abdullah and A. Al-Sayed (2020)- This paper explores the cybersecurity vulnerabilities in the financial sector. The authors discuss the threats posed by hackers, malware, and phishing attacks. They also examine the potential impact of these vulnerabilities on financial institutions and their customers. The authors argue that cybersecurity measures such as two-factor authentication and regular software updates can mitigate the risks.

Cybersecurity Vulnerabilities in the Internet of Things (IoT)" by M. A. Khan, A. Salah, and A. Al-Fuqaha (2019)-This paper examines the cybersecurity vulnerabilities in the Internet of Things (IoT). The authors argue that the widespread adoption of IoT devices has created new opportunities for cybercriminals. They identify various vulnerabilities, including weak passwords, unencrypted communications, and outdated software. The authors recommend that manufacturers implement security measures such as encryption and regular software updates to reduce the risks.

J. Graham, J. Hieb and J. Naber, (*2016)* examines the cybersecurity vulnerabilities in industrial control systems (ICS). The authors argue that ICS vulnerabilities pose a significant threat to critical infrastructure such as power grids and water treatment plants. They identify various vulnerabilities, including outdated software, weak passwords, and inadequate access controls. The authors recommend that organizations implement security measures such as intrusion detection systems and regular software updates to reduce the risks

A third challenge is the difficulty of balancing the need for security with the need for accessibility and convenience. This is highlighted in a study by Klievink and Janssen (2009), which argues that e-governance systems need to be designed with both security and usability in mind.

Chapter-3

3.0 Methodology

3.1 Research Process

There are four stages to the research process of this study (figure 1). The research began with defining the study's purpose, objectives, and scope, followed by a comprehensive literature review on the concept of cyber security, E-governance, Services by public administration and the formulation of research questions and objectives. The second step was data collection, which involved selecting a representative sample through a questionnaire.

The third phase is data analysis, which includes answering research questions, and commenting on the findings on data analysis in order to achieve the objectives set forth in the first phase. Finally, the fourth phase includes conclusions and recommendations.

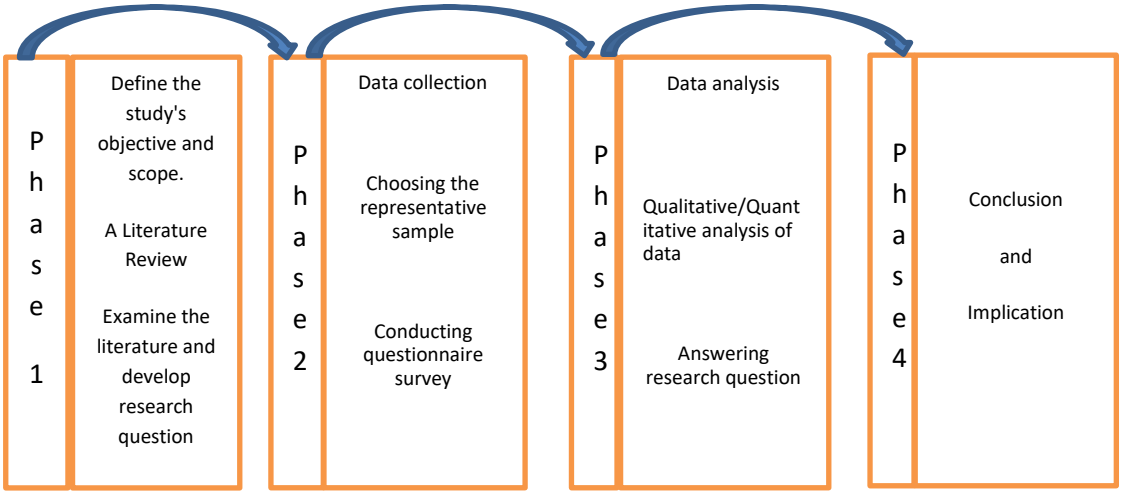

Figure 1: Research Process

3.2 Research Approach and Justification

The methodological approaches are qualitative, quantitative, or a combination of both uses for conducting research. This research will follow mix method because the primary purpose of this research is to identify the challenges, threats and to know the level of awareness regarding cyber security. The qualitative approach will help to clarify what the respondent said, to go beyond a convincing argument and to learn how it was promoted with an emphasis on the interpretation that derives from the contexts of the phenomenon. At the same time the

Quantitative methods will be apply to quantify data collection and analysis procedures suitable for measuring behavioral attitude.

Quantitative research deals with quantifying and analyzing variables in order to get results. It involves the utilization and analysis of numerical data using specific statistical techniques to answer questions like who, how much, what, where, when, how many, and how. It also describes the methods of explaining an issue or phenomenon through gathering data in numerical form. The study further reveals that quantitative methods can be categorized into; survey research, correlational research, experimental research and causal-comparative research.

3.3 Research Strategy of the Study

This study will follow the survey research strategy to collect & analysis data. The survey research strategy collects knowledge about research subjects by answering the same questions and documenting the findings of the survey into a chosen representative sample of the population, (i.e., people, communities, applications, initiatives, processes, and organizations). This takes a qualitative approach, gathering data through interviews and pre-designed questionnaire strategies with purpose, procedures, and analysis characteristics. It provides researchers with a quantitative description of the selected research population, including information gathering steps, and statistically analyzes the relationship between structures and compares and contrasts respondents' answers.

Considering the characteristics, the survey research strategy is chosen and is appropriate for this research due to assessing challenges of cyber security of different public offices.

3.4 Sampling and Study Area

A sample is "a group of smaller cases selected by a researcher from a larger sample library and generalized to the population. According to Kothari (2004), it's impossible to study the whole targeted population, and therefore, the minimum sample size in the survey situation and other statistical methods available should be determined in order to generalize population findings.

This study's sampling procedure will be broken down into several steps: identify the population, choose the sample frame and unit, choose the sampling method, and figure out the sample size. Sampling techniques include several considerations: necessity, time, effectiveness, and cost constraints. The preliminary sample framework of this research study

consists of all types of public offices rendering public services of Bangladesh Govt. This research will use stratified random sampling technique.

In selecting the best sample size, Roscoe (1975) stresses that it is optimal for the majority of study studies between 30 and 500. The sample size of this study will be at least 100 and 3 FGD groups (Head of the office, IT staffs, specialized govt. body on IT services and common employees). This study will be carried out in Bangladesh. The research team will visit 3/4 district level offices, 7-10 directorates (like Bangladesh computer council, BD e-GOV CIRT, Bangladesh Data Centre Company limited (BDCCL), Bangladesh Telecommunication Company Ltd. (BTCL) etc.) and if necessary team will visit other offices also. Focus Group Discussion (FGD) will be carried out in the Dhaka only.

3.5 Data Collection Methods and Techniques

The study will utilize mix method for data collection. Primary data will be obtained using questionnaires and FGD. Secondary data will be sourced from reading literature.

3.5.1 Survey Questionnaire

A structured questionnaire of quantitative nature has been used for the survey to identify the threats, vulnerabilities, steps taken to secure & develop the awareness among the government officials. Participants have got the opportunity to answer the questions by putting tick marks. In addition, the questionnaire encompasses some unstructured questions requiring descriptive answers of qualitative nature where the respondents have got the opportunity to put their opinion also. A total of 150 survey questionnaires were distributed and responses were received within March, 2023.

3.5.2 Focus Group Discussion (FGD)

Focus group research is “a way of collecting qualitative data, which—essentially—involves engaging a small number of people in an informal group discussion (or discussions), ‘focused’ around a particular topic or set of issues” (Wilkinson, 2004, p. 177). Focus group data can arise from one of the three types: individual data, group data, and/or group interaction data (Duggleby, 2005). It is a form of qualitative research where questions are asked about their perceptions attitudes, beliefs, opinion or ideas. FGDs are a good way to gather in-depth information about a community’s thoughts and opinions on a topic. The course of the discussion is usually planned in advance and most moderators rely on an outline, or guide, to

ensure that all topics of interest are covered (Parker & Tritter, 2006). Three FGD were conducted in this research with 24 participants who are the IT officials of the different public offices.

3.5.3 Document Analysis

For the study, the necessary secondary data has been gathered from a range of publicly available papers, journals, and reports etc.

3.6 Questionnaire Design

We have developed the questionnaire after a comprehensive analysis of literature. After developing the draft questionnaire, we have consulted with two renowned university professors from United American University (UIA) & University of Dhaka (DU) for removing, modifying and inserting appropriate questions (Churchill, 1979; Zikmund et al.,2010).

The questionnaire was split mainly into three parts: (1) instructions in a brief preamble; (2) General Information which deals with respondent the demographical data in part one. (3) The research study constructs data in part two to part seven , consisting of the factors which deals with information & network security and compliances of general awareness factors including data protection, password protection, monitoring, training etc. Part two deals with Antivirus Software, Anti-Spyware the network security challenges & Firewall etc. which represents; network security; part three deals with Software Development/ Vulnerability (vendor related) which represents cyber vulnerability; part four deals with Password Protection which represents the matter regarding computer security; part five deals with data protection; part six deals with monitoring & training and lastly part seven deals with cyber-attack & legal compliances. There were 50 questions in the questionnaire.

3.7 Ethical Consideration

The study has given thoughtful attention to ethical issues. Research ethics is concerned with the codes and principles research. Participation in this study was completely voluntary, respondents had the choice to skip question they felt uncomfortable or terminate the interview at any time. Consent of the interview was taken. All the data was kept in a secure place.

Chapter-4

4.0 Data Analysis

The questionnaire is used to examine 150 samples of the population of all types of public offices using disproportionate stratified sampling techniques. The online questionnaires and manual questionnaires are all designed and distributed to relevant employees of each public office via email, mobile phone, and physically. Total 106 questionnaires were returned. The response rate is 70.67%.

4.1 General Individual's Demographic Information

The general individual's demographic details were analyzed on the basis of gender, age, level of education, organization type, position and number of digital services. The demographic results showed that the majority of the sample were male (88.68%, 94) and the minority were female (11.32%, 12); the majority were between 31-40 years old (62.26%) and between 41 - 50 years old (25.47%) and the minority were 20-30 years old (9.43%) and 50+ (2.83%) of the population.. The study sought to determine the respondents' level of education. The majority held Master's degree or higher (57.55%); the Bachelor degree holders were 27.36% and others were 15.09% of the population. Among them, 35.85% are working in the Field Offices; 34.91% are the employees of Ministries and 29.25% works at Department level public offices. Again among the respondents, 89.62% were from ICT cell, 7.55% from General Employee (Administrative) and other were 2.83%. They were asked about the number of digitalized services of their organization and the answer showed that 1-3 services were digitalized in 20.75% offices, 3-5 services were digitalized in 16.98% offices and more than 5 services were digitalized in 62.26%.

Questions in part 2-7 deal with cyber security challenges on the network security challenges (Antivirus Software, Anti-Spyware & Firewall etc.), on cyber vulnerabilities {Software Development/ Vulnerability (vendor related)}, on computer security (Password Protection), on data protection; on monitoring & training and on cyber-attack & legal compliances . There were 43 questions in these parts of the questionnaire.

4.2 The network security challenges (Antivirus Software, Anti-Spyware & Firewall etc.):

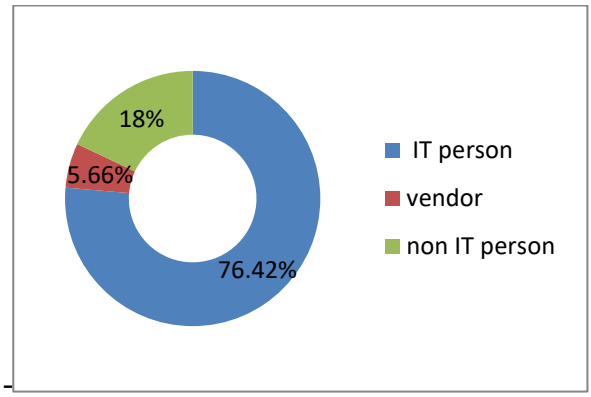

Figure-1: Responsible person for maintaining security software

The data analysis showed that person responsible for installing and maintaining security software in the computer/laptop/server, 76.42% were IT person, 5.66% were vendor and about 18% were non-IT person which indicates that there was still lack of IT person in public offices & this is also causing difficulty to maintain the network security.

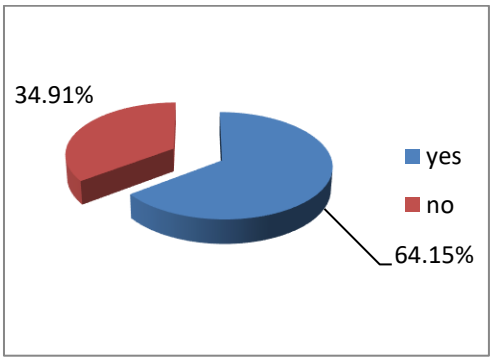

Figure-2: Use Licensed Software

Using licensed & updated software ensures to improve computer security. It was found from the data analysis that 64.15% offices use licensed software and update regularly, 34.91% don't which indicate that there is some gaps in ensuring network security in our public offices. Computer software needs to be updated regularly in order to be updated with standard configurations. Some organizations prefer carrying out just major updates while the others regularly conduct each and every windows update.

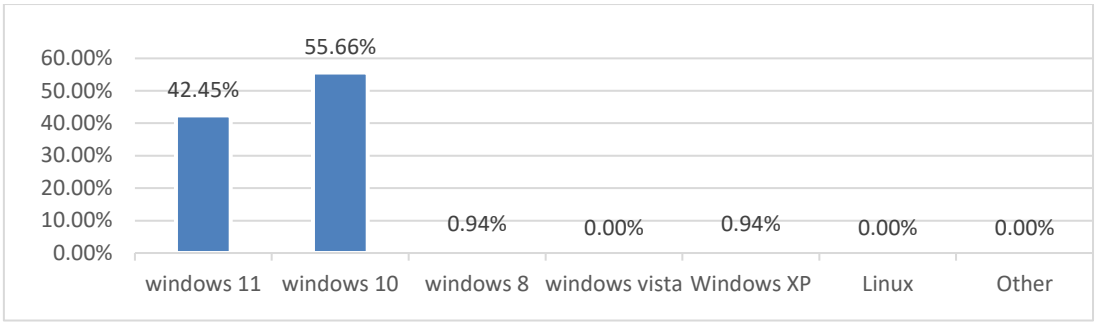

Figure-3: operating system is installed

The latest windows or any other software update will have the least number of issues. A computer needs to be updated regularly in order to be updated with standard configurations. Data shows that 55.66% organizations use ‘Windows 10’ & 42.45% use ‘Windows 11’. These are the updated version of operating windows.

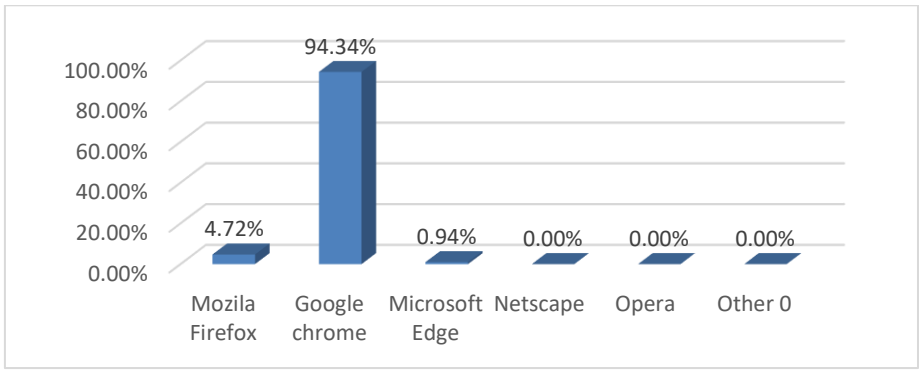

Figure-4: web browser use

Web browser can help organizations to understand whether their computer system is prone to security breaches via the web browser or not. 94.34% organizations use Google chrome; only 4.72% use Mozila Firefox and very few use Microsoft edge (0.94%).

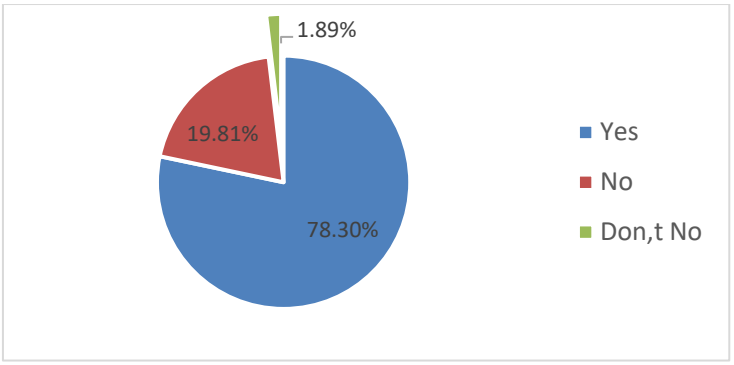

Figure-5: Use Anti-virus Software

It is essential for each computer to have antivirus software installed to keep computer virus free. Data analysis shows that 78.30% organizations use anti-virus software, where as 21% do not use which indicates that 21% organization's computers are in security threats.

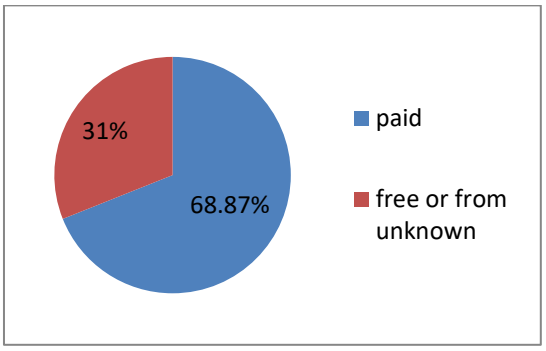

Figure-6: Anti-virus Software used from Free or Paid source

The respondents were asked about the software their organization uses paid or free; the result found that 68.87% were paid whereas 31% were free or from unknown sources; it indicates that 31% organizations have security problems. There are many reputed antivirus software available in the market. Each one has its one pros and cons and a business manager would know that. The organizations should use legal software which are paid. Though some use from free/unknown sources or downloaded from open sources which might cause threat to computers/laptops.

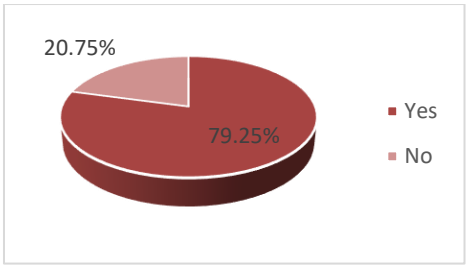

Figure-7: Anti-virus Software updates regularly or not

Every factor related to the computer must be updated regularly. An antivirus is one such factor which needs to be regularly updated. Outdated antivirus software may not work as shield to the computer protection.79.25% organization updates their antivirus software regularly & 20.75% do not regular basis.

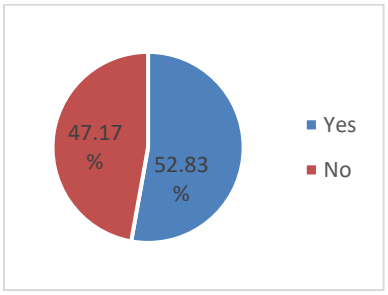

Figure-8: organization perform backup and restoration procedures on a regular basis

The analysis also shows that 52.83% organizations perform backup and restoration procedures on a regular basis to verify that viruses are not corrupting the backup data, 47.17% organizations do not do this on regular basis. The purpose of the backup is to create a copy of data that can be recovered in the event of a data failure. Data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data. so it is also important to check up regularly that back up data is not corrupted by viruses.

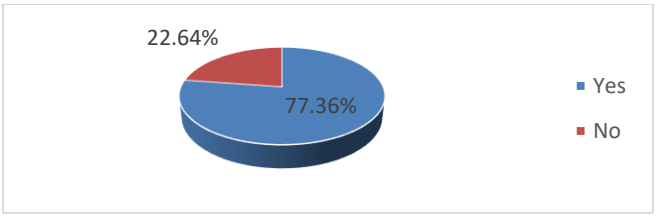

Figure-9: use internet security options in computers

Again, 77.36% organizations use internet security options in computers and 22.64% do not use. Internet security is critical because it prevents cybercriminals from gaining access to valuable data and sensitive information. When hackers get hold of such data, they can cause a variety of problems, including identity theft, stolen assets and reputational harm. So in our public offices, there are 22.64% offices are in vulnerable position for not using internet security.

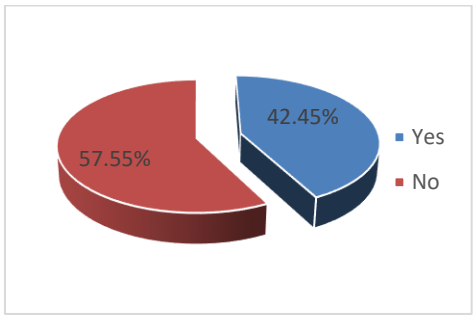

Figure-10: use Ad-blocker

Ad-blocker is a simple way to block annoying ads that make your browsing experience worse. Those ads mess large parts of websites, slow downloading speeds, and might be sources of malware. This study data analysis shows that only 42.45% Government offices use Add blocker in the browser and 57.55% do not use. So, more than half of the office's computers are in the position of getting threat of malware attack.

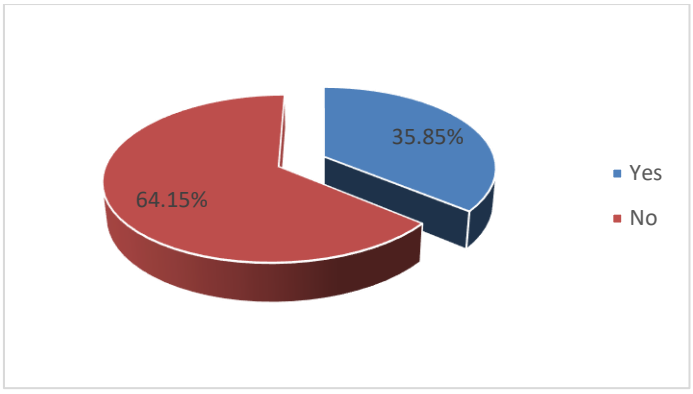

Figure-11: organization provide remote access to the servers installed

35.85% organizations allow remote access to the servers installed and 64.15% do not which indicates that 35.85% organizations/public offices are under threat of spyware attack.

4.3 Software Development/ Vulnerability (vendor related)

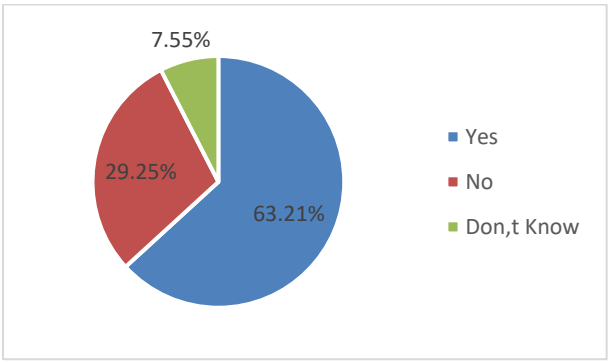

Figure-12: use firewall in LAN

The firewall may protect a poorly secured network from external threats. Their use across the firewall can be prevented, while use inside the firewall is allowed. Firewall provides boundary service to the LAN network, making sure that all connection to and from the internal network passes through the firewall. 63.21% offices ensure security using a firewall in their local area network whereas 29.25% offices do not use any firewall and 7.55% offices do not know about the matter. So, more than 35% public offices are in poor position regarding network security.

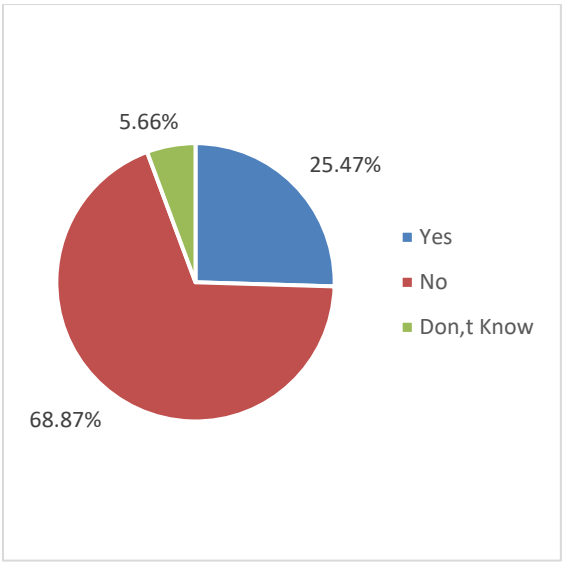

Figure-13: administration (Higher Authority) monitoring your computer all the time

Computers of an office need to be monitored exhaustively by the administration to ensure that whether security issues are regularly addressed or not. Monitoring ensures that the responsible persons are active to secure the network/computers/laptops/LAN etc. the pie chart shows, 25.47% respondents said that the administration monitor the computer to ensure security, but the majority (68.87%) said that the administrations do not monitor & 5.66% said they do not know about monitoring.

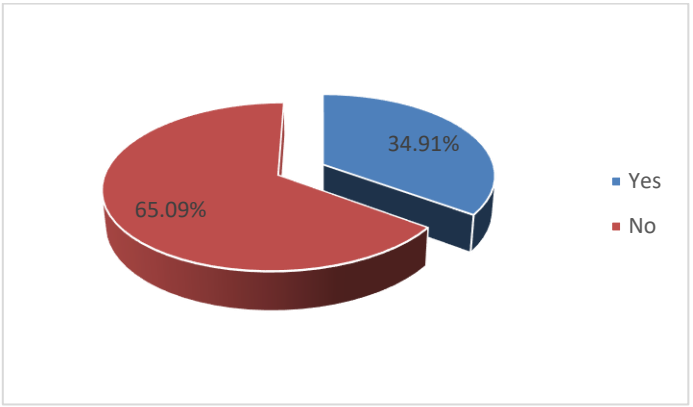

Figure-14: have backup personnel

The person behind ensuring security of data/information need to be identified and that person should be trained properly in relation to their duties, otherwise there may happen disaster/damage. The chart shows that 34.91% have their esteemed personnel and they are trained but majority i.e. 65.09% said they do not have. So, it can be draw conclusion from here

that in our public offices need to be designated dedicated personnel for ensuring discharging duties on computer security.

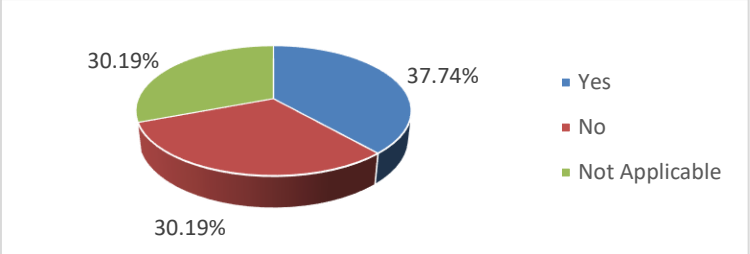

Figure-15: vendors need to notify on suspected information

Sometimes, the offices hire vendors or service providers to oversee the computer/network security matters. So, it should be cited in the contract with vendors to notify the organization immediately of a known or suspected compromise of customer information. The above pie chart shows that only 37.74% said that vendors need to inform offices, 30.19% said that no need to inform and 32.08% said that this is not applicable for them.

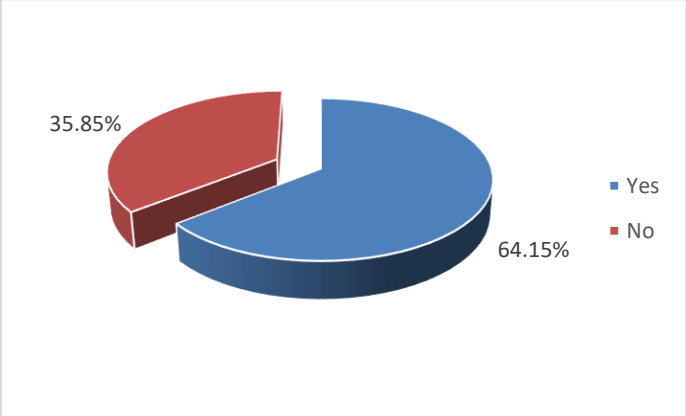

Figure-16: SSL certificates use

SSL certificates are used to create an encrypted channel between the client and the server. Transmission of such data as credit card details, account login information, any other sensitive information has to be encrypted to prevent eavesdropping. With an SSL certificate, data is encrypted prior to being transmitted via Internet. Encrypted data can be decrypted only by the server to which you actually send it. This ensures that the information you submit to websites will not be stolen. (What is an SSL certificate – Definition and Explanation, access

on 3/3/2023, https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate) The above pie chart shows that 64.15% offices use SSL certificates to ensure security in the application software and 35.85% offices do not use SSL certificates.

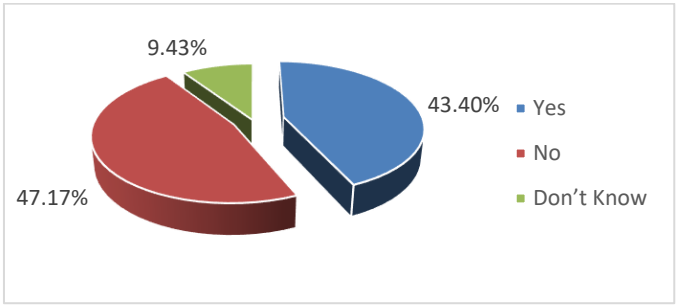

Figure-17: vulnerability check (VPAT/SQTC)

SQTC provide quality to the IT/ITES Industry if required to assure overseas clients. Besides, SQTC quality ensures that the applications are free from bugs and malicious code. The purposes of testing are quality, verification, and validation or reliability estimation.n On the other hand, VAPT stands for Vulnerability Assessment & Penetration Testing. It is a security testing to identify security vulnerabilities in an application, network, endpoint, and cloud. Both the Vulnerability Assessment and Penetration Testing have unique strengths and are often collectively done to achieve complete analysis.

The above pie chart shows that 43.40% offices test vulnerability with the tests VAPT and SQTC whereas 47.17% offices do not test and 9.43% respondent do not know. So, about 56% office's software may be vulnerable and there may arise cyber security problems.

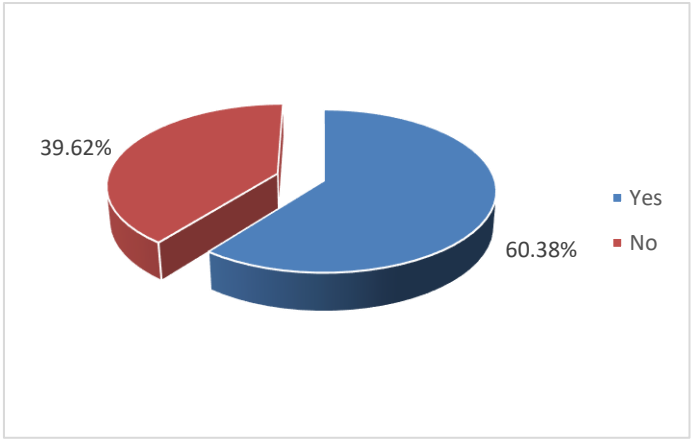

Figure-18: patch update regularly

Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. These patches help improve the performance of the software. Software updates may help fix bugs before they happen. By not updating or patching your software, your apps become more vulnerable to threats. The above chart indicated that 60.38% offices update their software patches regularly and 39.62% do not that means their software are in vulnerable positions.

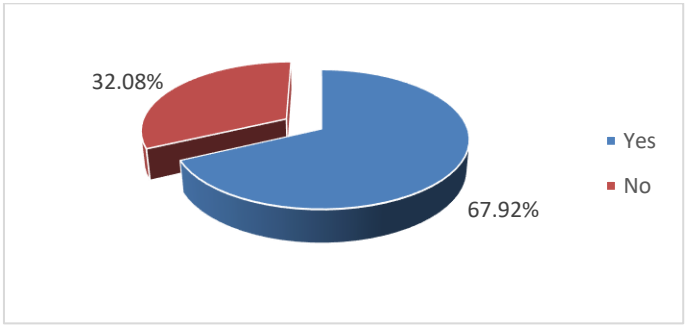

Figure-19: Capcha or Two factor use

Two factor authentication is essential to web security because it immediately neutralizes the risks associated with compromised passwords. If a password is hacked, guessed, or even phished, that's no longer enough to give an intruder access without approval at the second factor, a password alone is useless. According to the pie chart above, 67.92% offices use Capcha or Two factor authentication methods before logging in to the application software and 32.08% offices do not use which indicates that there may arise vulnerabilities in their web security.

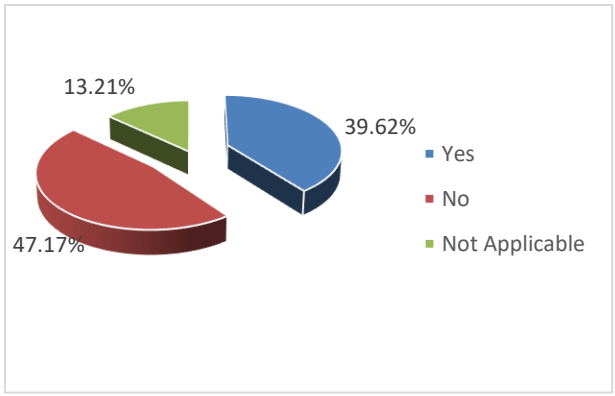

Figure-20: vendors access to the network

If any organization/office allows the remote vendor access to the network, then there will be two different users that means, authorization may not be under direct control of the office and perhaps there exists two different security policies which make the job of security compliance a challenge. So, vendors should be allowed to access with the presence of entrusted personnel. The data analysis shows that 39.62% offices allow the remote vendor access to their network which indicates of security challenges and 47.17% offices do not allow means they are cautious about the security.

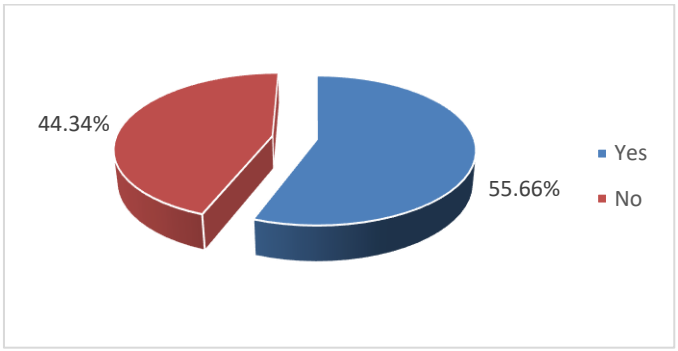

Figure-21: use piracy software

Using or distributing pirated software constitutes a violation of software copyright law. Piracy software might infect devices with viruses, malware, or adware. The above pie chart indicates that 55.66% offices use piracy software which means their computers or devices is on vulnerability with chance of infection with viruses, malware etc.

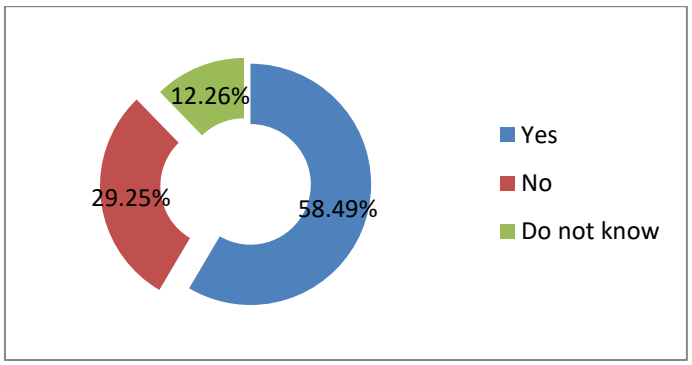

figure -22: Automatically cut off system access once a vendor's engagement finish

Unauthorized access to the network of an office may make threat. So, an office should not allow vendors to access to network at once their duty have been come to an end. The data analysis shows above those 58.49% offices automatically cut off system access once a vendor's engagement is complete and 29.25% offices do not cut off automatically which means they

need to come to agreement. 12.26% do not know the procedure. The last two indicate that vendor may access authorize to the network.

4.4 Password Protection

Password security is important because passwords are the first line of defense against cybercriminals and their unauthorized access to your personal data. A password protects your identity because it verifies that you are who you say you are. The following chart shows that 80.19% public offices use user ID and password to access to the computers whereas 16.98% offices do not use which means that computers may be affected anytime with cyber criminals.

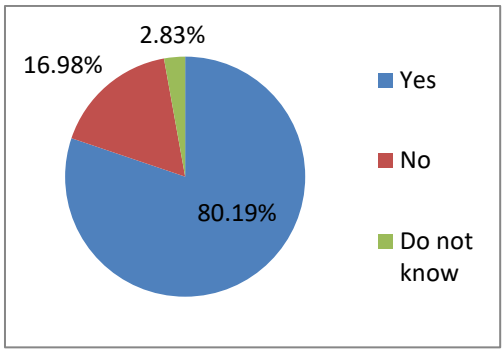

figure -23: using user ID and password to access computer

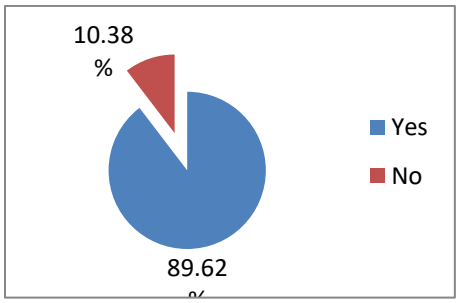

figure -24: Using same password

Security experts recommend using strong, unique passwords for each of your accounts to protect against common cyber-attacks. One should avoid reusing passwords. If accounts are compromised, cybercriminals can do a great deal of damage, such as committing identity theft, or stealing money and sensitive information from your place of work. The chart above shows that 89.62% offices do not use the same passwords as used in desktop and laptop computers to

protect the routers, wireless access points, switches and firewalls. Only 10.38% offices use same passwords which is detrimental for their laptops/computers they use.

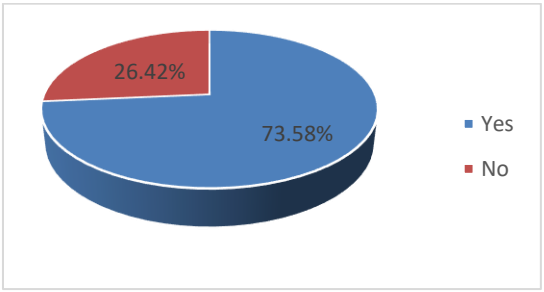

figure -25: password changed regularly

Strong passwords are of the utmost importance. They protect electronic accounts and devices from unauthorized access, keeping sensitive personal information safe. The more complex the password, the more protected your information will be from cyber threats and hackers. Regularly updating passwords means that even if someone finds an old or saved password, it will no longer be useful, and data will be secure. 73.58% offices change their password regular basis where as 26.42% offices do not do this.

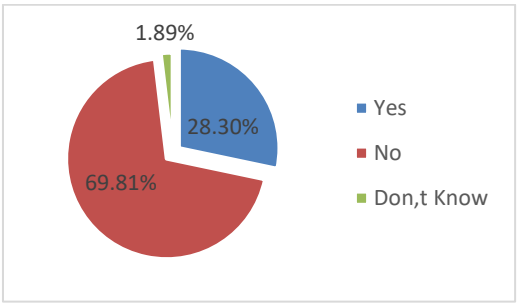

figure -26: Wi-Fi password share to strangers

If anyone gives a password to one person, they might give it to a number of people after that, increasing the risk that your IP address will be used for unlawful activities. A trusted neighbor might not misuse your Wi-Fi, but a stranger might perceive it as an opportunity. In these cases, hackers were able to breach security that was put in place and steal customer information from the network. This type of data breach could be catastrophic for a small business. So, an office/organization should not share their wi-fi password. 28.30% public

offices share their Wi-Fi passwords which is threat to their network. 69.81% offices do not share their passwords and 1.89% offices do not know.

4.5 Data Protection

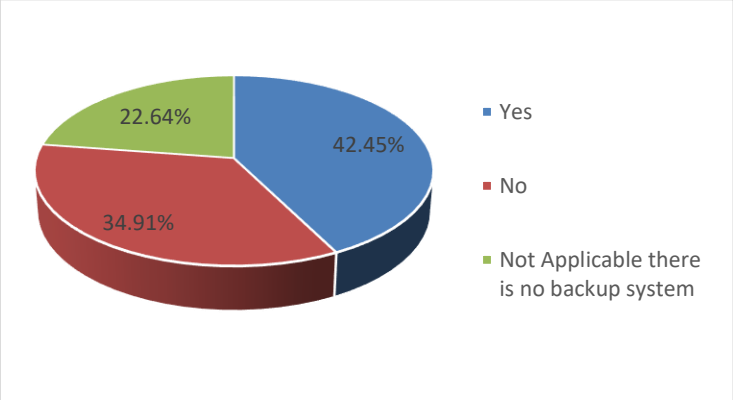

figure -27: encrypting backup data storage

Encryption is a powerful tool to keep sensitive data out of the wrong hands. To ensure recoverability after a disruption, data backup encryption is vital. The key to data integrity is reliability and trust at all times. Backups are a vital part of data and application recoverability and must always be secure. 42.45% offices encrypt its backup data storage devices; 34.91% offices do not encrypt and 22.64% offices have no back system.

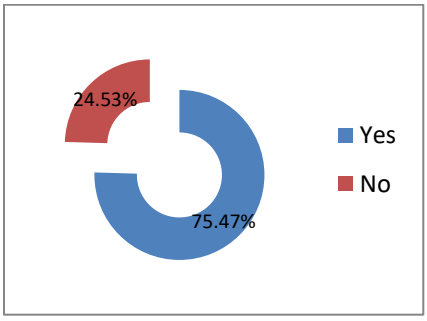

figure -28: Hosting software in National Data Center

Data centers provide services such as: Data storage, management, backup and recovery. It provides a secure place to store online content. 75.47% offices hosted their software in National Data Center/ BDCCL (Bangladesh Data Centre Company Ltd) and 24.53% do not hosted in the National Data Center/ BDCCL; they may keep their data in their own storage which might not be safe and be easy to access for the cyber criminals.

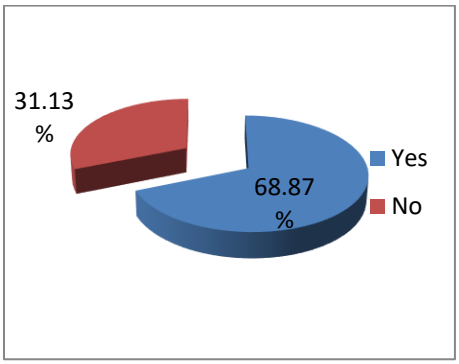

figure -29: Obtained source code

The source code of the developed software, database, required credentials and documentation should be obtained from the vendor organization otherwise anytime the vendor may exploit the software for negative purpose which brings devastating effect to information of host organization. There is direction for the government offices of Bangladesh to obtain source code of the developed software. 68.87% offices follow this direction and 31.13% still do not maintain the direction which might be harmful for them.

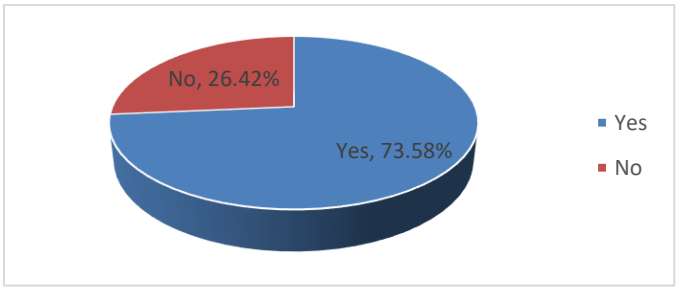

Figure-30: following BNDA guidelines

BNDA (Bangladesh National Digital Architecture) has been developed to synchronize the transformational potential of technology; it ensures interoperability among the various services of the Government. (https://bnda.gov.bd//page/nda-details.jsp). It is asked to the respondents whether their office/organization follow the BNDA guidelines to develop software. The data shows that 73.58% offices follow BNDA guideline and the rest (26.42%) do not follow which means their service may not be compatible for interoperability.

4.6 Monitoring & Training

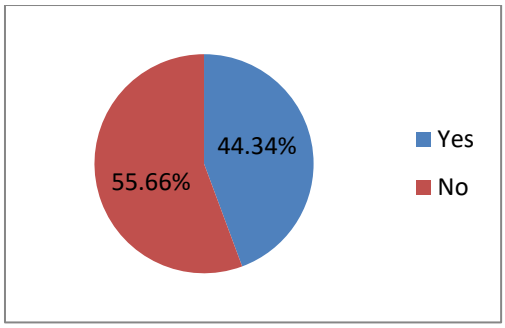

Figure-31: Have intrusion detection system

An intrusion detection system (IDS) is software that checks a network or system for malicious activities or policy violations. IDS monitor a network or system for malicious activity and protect a computer network from unauthorized access from users, including perhaps insiders. Every organization should have a process for intrusion detection system. The following chart shows that 44.34% offices have their intrusion detection system (IDS) and employees are trained to monitor intrusion properly. 55.66% offices do not have which their computer network or system may be attacked by malicious activity and unauthorized access from users.

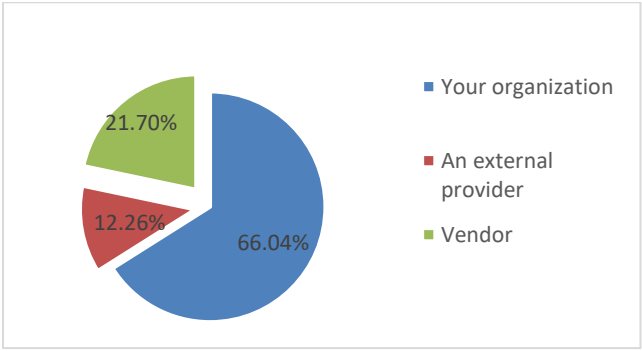

Figure-32: looks after the system security

Data analysis shows that 66.04% offices look after their system security and managed by them. 12.26% office's system security is looked after by an external service provider and 21.70% office's system security is looked after by vendor management. So, there is chance of arising security question on about 34% office's system security.

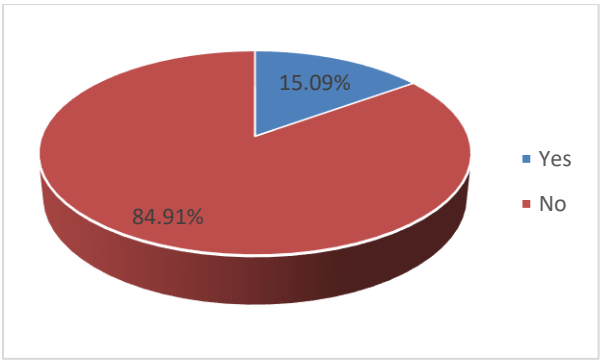

Figure-33: allow a stranger to use laptop or server

If an organization allows a stranger, it may bring threats to its system security. In these cases, hackers were able to breach security that was put in place and steal customer information from the network. This type of data breach could be catastrophic for a small business. So, an office/organization should not allow using its desktop, laptop or server. 15.09% respondent said that they allow stranger to use their computer which is dangerous for their security of information. 84.91% offices do not allow strangers to use their desktop, laptop or server.

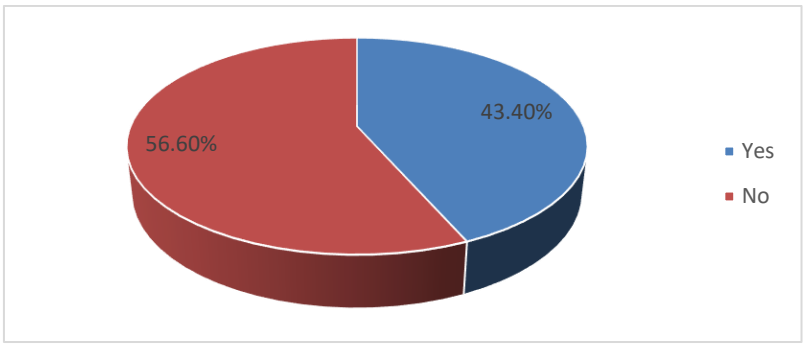

Figure-34: regularly refrain from using pre-proxy sites

Attackers can easily intercept communications over unsecured proxies, meaning any sensitive data like usernames and passwords are at risk of being compromised. Unsecured connections also put users at high risk of data breaches, such as identity theft. An organization should refrain its user from using pre-proxy sites. In case of our public offices, 43.40% offices refrain regularly and 56.60% not in regular basis.

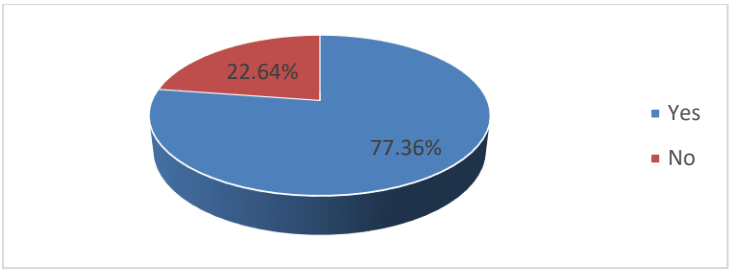

Figure-35: top management support the IT team

Top management support i.e. decision makers of an office are very much important to ensure cyber security. If do not support or understand the consequence of cyber threats then this may cause problems for that office. Data shows that 77.36% respondent said that their top management support the IT team in matters like budgeting, decisions, etc. for system security whereas 22.64% said that top management do not support properly/as expectation.

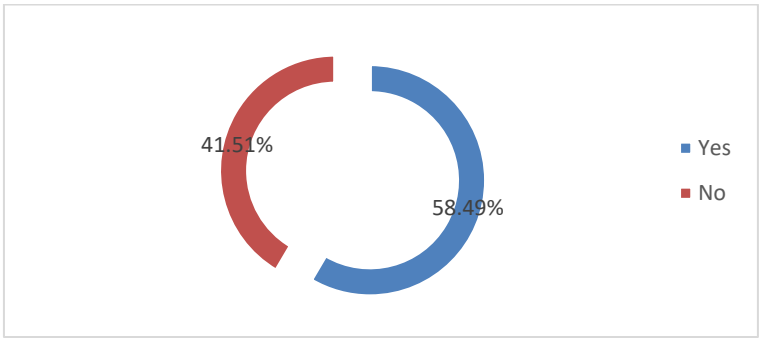

Figure-36: cyber security in training module

An organization should include cyber security matter in its training module for its employee awareness and knowledge. 58.49% respondents said that cyber security awareness and techniques included in the training module & 41.51% said not included which indicate cyber security may be issue for them.

4.7 Cyber Attack

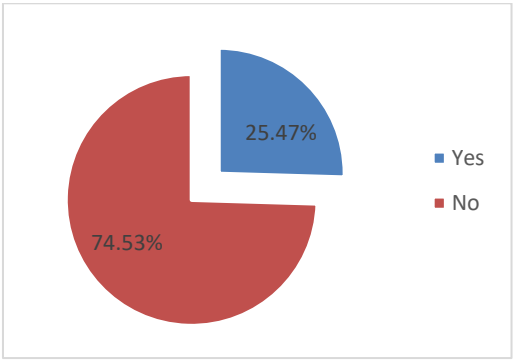

Figure-37: Attacked by clicking on untrusted links

Unsafe links/domains are external links to websites that could contain phishing, malware, or unwanted software. Safe Links checks URLs to see if they are malicious or safe before loading the web page. Data analysis indicates that 25.47% respondents have clicked on untrusted link and they attacked for that and 74.53% respondents are aware of clicking untrusted links.

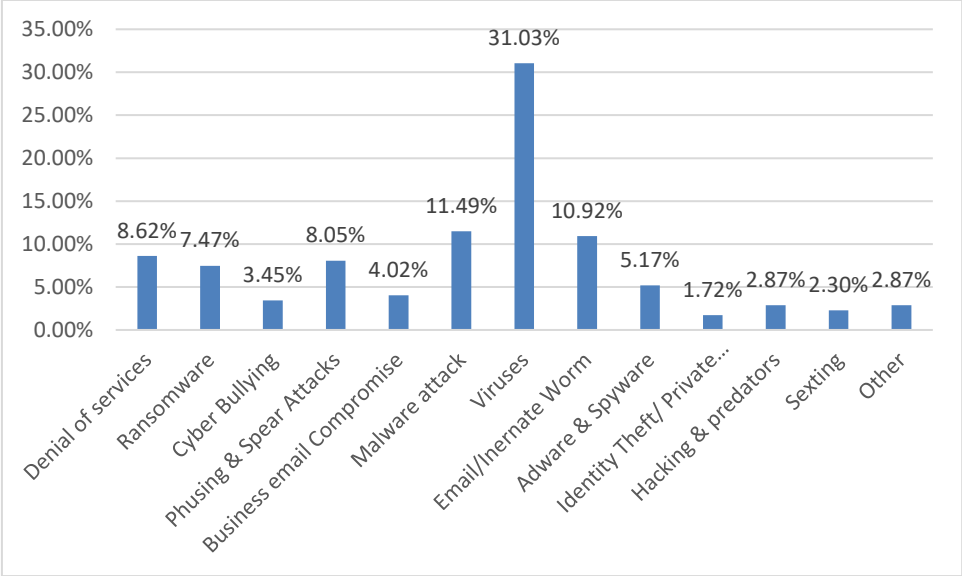

Figure-38: cyber-attack experience

The threats which are faced by our public office so far as Denial of Service (DoS) (8.62%) ransomware (7.47%), Cyber Bullying (3.45%), Phishing and Spear Attacks (8.05%), Business Email Compromise (4.02%), Malware Attack (11.49%), Viruses (31.03%), Email/internet Worm (10.92%), Adware and Spyware (5.17%), Identity Theft/ Private information (1.72%), Hacking

and predators (2.87%), Sexting (2.30%) and Other (2.87%) types of threats. Maximum attacks are faced viruses attack.

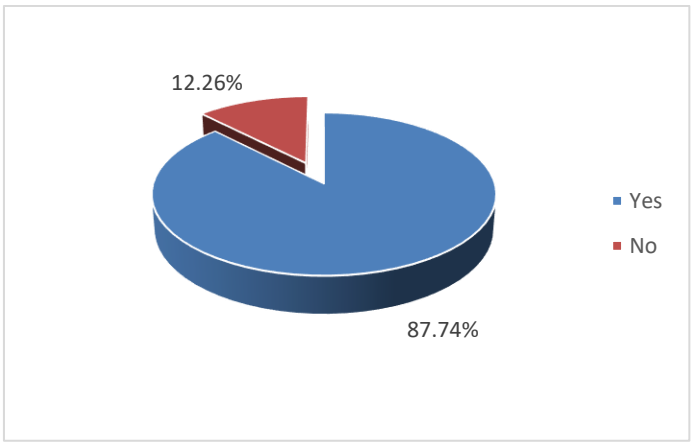

Figure-39: official e-mail use

It is safe to use Government official e-mail of a public office. 87.74% respondents said that they use the official email and 12.26% said that they do not use the official email. Personal email Vulnerabilities in transmission. This email is not protected by work IT security team. Personal emails have no backup. Official email accounts have a upgraded protection that standard personal ones do not.

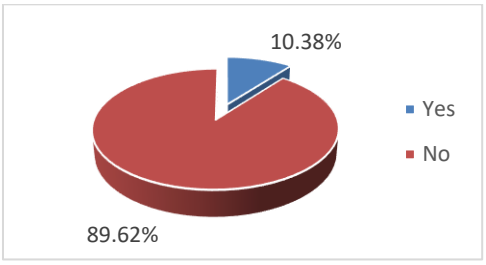

Figure-40: open suspicious e-mails

Documents attached to suspicious e-mails cause phishing attack. 10.38% respondents said that they open the documents attached to suspicious e-mails and 89.62% said that they do not which indicates they are aware about using e-mails.

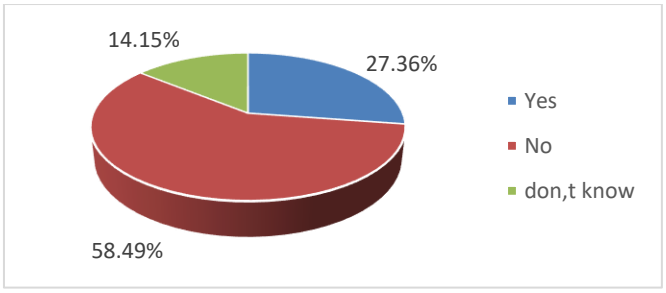

Figure-41: firewall allow downloading pirated video

A firewall is a necessary safeguard for any online network. Firewall primarily prohibits to use untrusted contents like pirated videos. 27.36% respondents said that their organization's firewall allow downloading pirated video or other contents which may bears threats for information security and 58.49% said that they do not allow. Other 14.15% said that they do not know.

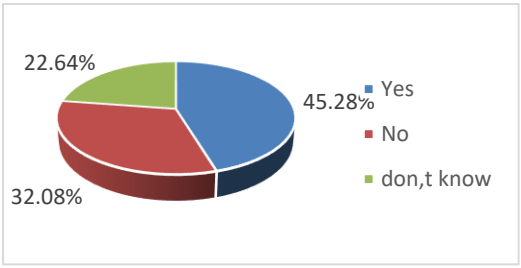

Figure-42: allow USB to computer

Malicious USB drives have pre-programmed malware that enables attackers to access the victim's peripherals, including the keyboard, get network access and move laterally to different computer systems, steal confidential information, and observe network activity for the organization. 45.28% respondents said that their organization allows to use USB to official laptop/computers/server which may bear threats of cyber security and 32.08% said that they do not allow and 22.64% said that they do not know which is also ignorance of cyber security consequences.

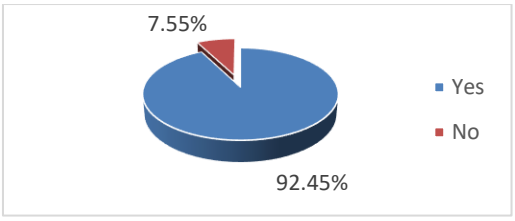

Figure-43: follow Government e-mail policy

It is safe to use Government official e-mail of a public office. 92.45% respondents said that their office follows the official email policy and 7.55% said that they do not follow the official email policy. The above statistics indicates that remarkable security issues prevail in Government offices of Bangladesh to render public services.

4.7 FGD Analysis

Two FGD were conducted in this research with 22 participants who are the IT officials of the different public offices. The FGD participants stressed on 3 pillars i.e. people, process and technology. They mentioned the people which include security employee awareness, behaviour & training, Specialist skills, experience, qualifications & sufficient staff; The process which includes appropriate policies, management systems, frameworks of cyber security, planning, performing audit & reporting on audit findings; and The technology which includes network, infrastructure and platform security, endpoint security, detection and response, application and software security, vulnerability scanning and monitoring, advanced threat protection, identify and access management, managed security solutions and services, data security and protection & cloud security. They categorically discussed all these three pillars and identified the challenges of cyber security faced in Government sector service delivery. FGD participants emphasize on employee awareness building and trained people. If proper skilled people can be employed behind the cyber issues, most of the challenges can be mitigated. Another point came out from the discussion that the security system should be properly audited.

In the FGD discussion, participants discussed about various threats and causes of it occurring in government offices. They specially mentioned about ransomware and phishing. The vulnerability identified from their discussion that the software which are used in the public

service delivery sector, most of cases are not tested like VAPT/SQTC etc. The security systems are not also updated regularly with proper monitoring by the IT people. The participants mentioned, cyber security issues are happening because of not using licensed software, for not using in computers proper antivirus software even for using USB. Sometimes unauthorized person enters in the network and also use the Wi-Fi. They stressed on using strong password and not to share with any others as password hacking is one of the major causes of breaching cyber security or cyber-attack. Point came out from the discussion that updating of Firewall. Our IT persons & administration (Higher Authority) do not monitor updating of firewall. Keeping your firewall updated is a key aspect of protecting your network, computer system, and data. Old and aging firewalls pose a great security risk for your domain. For instance, a five-year-old firewall is typically 50 percent less effective at stopping cyber-attacks as compared to a two-year-old unit.

FGD participants focus on backup storage of information so that after Cyber attack it can be reset the system within short time. FGD of banking sector suggest to maintain Continuous collaboration, cooperation and threat information sharing among government entities to combat cyber threat. They also suggest that Software & Data also be stored for backup in disaster recovery site.

The data from the FGD revealed more or less same findings like survey questionnaire data findings.

Chapter-5

Study Findings

This study and its research objectives are to know the current challenges in cyber security in Government offices of Bangladesh, to identify the cyber security threats & vulnerabilities regarding digital service delivery and to make recommendations in relating to the cyber security. It is clear from the review of relevant literature that cyber security becomes a concern for digital service delivery due to various reasons. This study has tried to find out the objectives of this study by a survey questionnaire and Focus Group Discussion (FGD) from relevant government employees and responsible persons. The analysis of data achieved from survey questionnaire and FGD shows that in our public offices the main challenge is lack of skilled IT person (36%). Besides this, the software which are using in the offices, remarkable percent (35%) are not licensed, not using anti-virus software (22%) & those who are using, using more than 31% from free/unknown sources and at the same time they are not updating regularly (20.75%). Most of the public offices are not verify regular basis that viruses are not corrupting the backup data. These challenges are prevailing due incautiousness about cyber threats & its consequences.

Again, the public offices are not using internet security options in computers (22%) & not ensuring security using a firewall in the local area network (38%); even they are not ensuring to notify in suspected case by the vendor. The software which the offices are developed for rendering services, are not testing vulnerability (57%) and not using SSL certification (35.85%). Sometimes they are giving remote access to vendors (39.62%) and not using two factor authentication (32.08%), these things are creating challenge for ensuring cyber security in the system. There exist password related problems also. There is also gap in close monitoring and maintaining the government policy.

Our IT persons & administration (Higher Authority) do not monitor do not monitor computer seriously. In analysis 25.47% respondents said that the administration monitors the computer to ensure security, but the majority (68.87%) said that the administrations do not monitor & 5.66% said they do not know about monitoring.

firewall updating is another problem. 63.21% offices ensure security using a firewall in their local area network whereas 29.25% offices do not use any firewall and 7.55% offices do

not know about the matter. So, more than 35% public offices are in poor position regarding network security.

The vulnerabilities are prevailing regarding software which are using in public offices are not developed as per the government BNDA guideline (26.42%), not SSL certified (35.85%) & not testing vulnerability (57%). The vendor are getting remote access and the source code remaining to vendors which are very risky for security issues. Sometimes Employees shares passwords to strangers and also using piracy software. The offices need to address these vulnerabilities properly.

From FGD in field level we found that many DC offices use redundancy line from ISP vendor who do not use any firewall. In local level hardware/computer/routers/laptops repairs by vendors who can create any cyber security risks for their gain. All dc offices use only pirated software for lack of budget and awareness which are vulnerable for cyber security. In each DC office has one or two IT person only who are not trained on cyber security. So in field level need more IT personnel who should be trained on cyber security.

Various cyber threats are being facing by the public offices due to lack of awareness, employees click on untrusted links (25.47%), open the documents attached to suspicious e-mails (10.38%), firewall of the office allows to download pirated video or other contents (27.36%), use USB to official laptop/computers/server (45.28%), shares passwords to strangers, use piracy software & allow vendor to remote access. The threats which are faced by our public office so far as Denial of Service (DoS) (8.62%) ransomware (7.47%), Cyber Bullying (3.45%), Phishing and Spear Attacks (8.05%), Business Email Compromise (4.02%), Malware Attack (11.49%), Viruses (31.03%), Email/internet Worm (10.92%), Adware and Spyware (5.17%), Identity Theft/ Private information (1.72%), Hacking and predators (2.87%), Sexting (2.30%) and Other (2.87%) types of threats.

Chapter: 6

Challenges

Bangladesh is experiencing various types of challenges to ensure cyber security. From this research some of the current challenges are observed in public offices in Bangladesh to ensuring cyber security which are discussed below:

1. **Pirated software:** Data analysis showed that around 60% of software are pirated. The use of pirated software is leading government office to get a more vulnerable position in the cyber security domain.

2. **Lack of awareness & sincerity among government employees:** Data analysis show that many employees are not aware & sincere of the importance of cyber security. General people also unaware about cyber security. Hence, lack of awareness & sincerity can lead to unintentional security breaches, such as the use of weak passwords or the sharing of sensitive information.

3. **Shortage of cybersecurity professionals' skills:** From FGD in government office there is a great shortage of cybersecurity professionals' skills which is a significant obstacle in developing effective cybersecurity policies and practices.

4. **Lack of Vulnerability Assessment and Penetration Testing (VAPT):** Lack of VAPT before hosting software to identify security vulnerabilities in an application, network, endpoint, and cloud.

5. **The increasing sophistication of cyber-attacks:** From data analysis found that increasing sophistication of cyber-attacks for rapidly changing of technology and use of ICT growing.

6. **Poor Infrastructure:** From FGD Most public offices in Bangladesh do not have robust IT infrastructure and data centers. Hence, the security of data is usually not adequate.

7. **Hardware maintains vendor dependent:** In field level hardware maintains depend on vendors who can create any cyber security risks for their gain.

8. **Weak backup server:** Data analysis around 30% public offices hosted their data on local server. Local servers are not standardized. Many of them have no backup server. These make great vulnerability for data protection.

9. **Lack of proper Monitoring**: From data analysis the majority (68.87%) said that the administrations (IT) do not monitor. Monitoring ensures that the responsible persons are active to secure the network/computers/laptops/LAN.

10. Lack of software audit. FGD suggest that regularly internally or externally software audit is necessary for ensuring licenses are up-to-date & identifying weaknesses of software. Otherwise, create a vulnerability for cyber threat.

11. **Rapid pace of technological change:** which can make it difficult for governments to keep up with the latest cyber security threats and solutions.

12. **Complexity of government IT systems:** Public administration systems often involve multiple departments, agencies and levels of government, which can make it difficult to ensure consistent and comprehensive cybersecurity measures across the entire system.

13. **Outdated Technology:** From FGD public offices in Bangladesh often use outdated technology and software, making them more vulnerable to cyber threats. The outdated systems may not have the latest security updates, which could expose them to malware attacks.

Chapter 7

Recommendation & Conclusion

7.1 Recommendation or Way forward:

The rapid growth of information and communication technology worldwide has made the potential of cybercrime worldwide even in Bangladesh. Bangladesh has already become vulnerable to cyber-attacks due to the inadequacy of ICT resources and a lack of skilled cybersecurity professionals to defend or protect its cyberspace. Now Cybercrime is increasing exponentially. From data analysis & FGD, the following recommendations that may be considered highly prospective to deal with cyber-attacks and cyber insecurities in Bangladesh:

1. **Awareness & sincerity build up:** From data analysis we have found that our IT administrator (higher authority) & other government officials are not aware & sincere regarding cyber security & cybercrime. All cyber-attacks have occurred in Bangladesh due to lack awareness & sincereness. So it is need intensify efforts at all levels of public offices to promote understanding of cyber risk & threats.
2. **Training on Cyber Security Issues:** the public offices should establish regular mandatory training for IT employees & general employees regarding cyber security issues.
3. **Professional training for IT person:** IT staff should be trained on cyber security issues professionally so that they can react to incidents as its occur.
4. **Enforce to follow password policy:** Public offices should enforce strictly to follow password policy for all kind of user access to devices, application & portal:
5. **Enforces to follow authentication:** Public offices should enforce strictly to follow two factor authentication/ multi factor authentication in terms of accessing all the sensitive application/ portals /emails.
6. **Latest Technology/devices:** All Public offices should use latest technology to mitigate latest cyber threats. (Example latest firewalls/routers/switches).

7. **Maintain updated software**: Public offices should regularly update software, security patches, and anti-virus software which can help to prevent cyber-attacks.
8. **Use license version software in place of pirated software:** Public offices should use License-version software/antivirus; prohibit & remove pirated software from public offices to keep computer/server/laptop virus free.
9. Virus scanning should be done before using USB flash drive.
10 **Appoint a cybersecurity officer:** Public offices should appoint a dedicated cybersecurity officer to oversee the implementation of cybersecurity measures that can ensure security protocols up-to-date and effective & reduce vendor dependency.
11 **Conduct regular cybersecurity assessments:** From FGD, it was suggested that regular assessments of the IT infrastructure should be conducted to identify vulnerabilities and assess the effectiveness of current security measures
12 **Create an incident response plan:** In the event of a cybersecurity breach, a well-defined incident response plan should be taken to minimize the impact of the attack and ensure that data and systems to be restored as quickly as possible.
13 **Data hosting in BDCCL & NDC:** Operating Software, Application software & data should be hosted in BDCCL & NDC server instead of local server. Software & Data also be stored for backup in disaster recovery site.
14 **SQTC & VAPT:** SQTC (Software Quality Testing and Certification Centre) and Vulnerability Assessment and Penetration Testing should be done before hosting software.
15 **Regular Audit:** Mandatory regularly internally or externally software audit is necessary for ensuring licenses are up-to-date & identifying weaknesses of software.
16 **Follow of policy guide line:** Government officials should properly follow the Digital Device, Internet & Information Security Guide Line, 2020 of Cabinet División, the government email Guidelines & BNDA guide to mitigate cyber risk & vulnerability.

17 **Comprehensive cyber security Strategy:** To face future challenges need a comprehensive cybersecurity strategy that addresses both technical and non-technical aspects of cybersecurity.

18 **Adequate budget:** Public offices should allocate sufficient budget for cyber security.

19 **Monitoring & Collaboration:** Continuous monitoring and collaboration, cooperation and threat information sharing are needed among government entities to combat cyber threat.

7.2 Conclusion:

As per Bangladesh's Perspective Plan 2021-2041, the country is expected to become developed by 2041. Again, according to the Smart Bangladesh Vision 2041, Inclusive digital transformation needed to build a developed and prosperous Country by 2041. In order to realize these visions, ICT will be essential. Because of this, the usage of computers and information technology is growing quickly across a range of sectors and levels of government, business, and industry. However, due to a lack of knowledge, a severe dearth of qualified cybersecurity experts, and outdated IT infrastructure, the danger of cyber security is rising. Cybersecurity is becoming risky for a nation's economy. So cyber security become a great concern & challenge in the world as well as in Bangladesh.

Every day, there are more and more cyberattacks. Regardless of size, no business can get rid of it. Over the previous several years, the number of impacted enterprises has nearly doubled. Bangladesh is digitizing all government operations at the moment. Both large and small organizations are growing used to utilizing technology. The shift is being exploited by cybercriminals. Ransomware assaults have escalated recently in Bangladesh. Nobody is immune to this malware—not even individuals or organizations. Malware- and phishing-based assaults are also becoming more frequent. Malware without files will rule the next age. Thus, we must exercise greater caution and awareness. People should be made more aware of cybersecurity. Organizations must appropriately abide by defense regulations. Everybody must create their own cybersecurity rules and safeguards.

References

- Adil Ahmed Chowdhury, Farida Chowdhury, Md. Sadek Ferdous, (2020). A Study of Password Security Factors among Bangladeshi Government Websites, 23rd International Conference on Computer and Information Technology (ICCIT), 19-21
- Farahmand F, Navathe SB, Sharp GP, Enslow PH. A Management Perspective on Risk of Security Threats to Information Systems, Information Technology and Management archive; 2005;6: 202-225.
- Jouini M, Rabaia LB, Aissa AB. Classification of security threats in information systems. Procedia Computer Sci; (32): 489-96. [http://dx.doi.org/10.1016/j.procs.2014.05.452]
- Chowdhury, A., and H. Zaman. 2014. "Embedding Innovation in Government's DNA: Lessons from Bangladesh." Information Technology in Developing Countries 24 (2): 9–12. Ahmadabad: Indian Institute of Management (IIM). Accessed January 30, 2015. http://www.iimahd.ernet.in/egov/ifip/ june2014/Bangladesh%20paper.htm
- 'WannaCry ransomware attack, (2017). accessed on 14/04/2023. https://www.bbc.com/news/technology-40194191
- U.S. Department of Justice. (2020). Cybercrime. Accessed on 18/03/2023. Retrieved from-https://www.justice.gov/criminal-ccips/cybercrime
- Bangladesh Telecommunication Regulatory Commission (BTRC), (2020). Annual Report 2019-2020, Accessed on 09/03/2023, http://old.btrc.gov.bd/sites/default/files/paper_files/BTRC%20English%20Annual%20Report-2019-2020.pdf
- Md. Mahbubur Rahman Alam. Md. Shihub Uddin khan & Kaniz Rabbi, (2023). Internet Banking in Bangladesh: Trust, User Acceptance and Market Penetration. Accessed on 09/04/2023. https://www.bibm.org.bd/publications-read.php?id=84
- Digital Information Security Guideline- (2017). Cabinet Division, Bangladesh.
- Making Vision 2041 a Reality PERSPECTIVE PLAN OF BANGLADESH 2021-2041, General Economics Division (GED), Bangladesh Planning Commission Ministry of Planning Government of the People's Republic of Bangladesh, March 2020.
- Available from: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=70E868EBB5E530CDA1AF059A22A5D485.1_cid341 [Accessed: 2018-01-10].

- UNDP, Public Administration Reform: Practice Note, pp. 1–2. Available from www.undp.org/content/dam/aplaws/publication/en/publications/democratic-governance/dg-publications-for-website/public-administration-reform-practice-note-/PARPN_English.pdf.
- Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security. ORP.3: Sensibilisierung und Schulung/Sensitization and training. Bonn; 2016. Available from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html [Accessed: 2018-01-17].
- UNDP, (2021), DIGITAL BANGLADESH TO INNOVATIVE BANGLADESH: THE ROAD TO 2041, access on 21/03/2023, https://www.undp.org/bangladesh/blog/digital-bangladesh-innovative-bangladesh-road-2041
- A K M Bahalul Haque, (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, No.1, February 2019. DOI : 10.5121/ijmit.2019.11103 37.
- Tushar P. Parikh et al. (2017). International Journal of Research in Modern Engineering and Emerging Technology, (IJRMEET) ISSN: 2320-6586Vol. 5, Issue: 6, June.
- Habib Zafarullah and Noor Alam Siddiquee (2001). Dissecting Public Sector Corruption in Bangladesh: Issues and Problems of Control, Public Organization Review 1(4):465-486. DOI:10.1023/A:1013740000213
- Bangladesh Cyber Threat Landscape (2021), “BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team |.” [Online]. Available: https://www.cirt.gov.bd/. [Accessed: 05/08/2022].
- Bangladesh Cyber Threat Landscape, (2020), “BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team |.” [Online]. Available: https://www.cirt.gov.bd/. [Accessed: 05/08/2022].
- Meier J, Mackman A, Vasireddy S, Dunner M, Escamilla R, Murukan A. (2003). Improving we application security: threats and counter measures. Satyam Computer Services, Microsoft Corporation; The Daly Star,

https://www.thedailystar.net/opinion/views/news/one-step-forward-two-steps-back-3073261, Accessed on date 25/08/2022.

- Aspire to Innovate (a2i), https://a2i.gov.bd/, Accessed on date 23/08/2022.
- Financial news, Dated 13/06/2022, https://funancial.news/more-than-half-of-banks-at-high-risk-of-cyber-attacks-bibm/, Accssed on date 25/08/2022
- Mohammad Nur Nabi & Muhammad Tanjimul Islam (2014), Cyber Security in the Globalized World: Challenges For Bangladesh; Economic And Social Development, 7th International Scientific Conference, New York City
- Muhammad Saifuddin Khan* Suborna Barua (2009), The Status and Threats of Information Security in the Banking Sector of Bangladesh: Policies Required Bangladesh, Journal of MIS, Vol.1, No.2, June 2009, ISSN: 2073-9737, Department of Management Information Systems, University of Dhaka.
- Islam, M. A., & Abdullah, M. S. (2019). Cybersecurity in Bangladesh: An Analysis of Current Status and Future Challenges. International Journal of Network Security, 21(2), 299-307
- Anir Chowdhury (2023), What is SMART Bangladesh is Really?, Accessed on 21/03/2023. https://a2i.gov.bd/what-is-smart-bangladesh-really/
- ISO. Information Processing Systems-Open Systems Interconnection-Basic Reference Model. Part 2: Security Architecture, ISO 7498-2; 1989.
- Meier J, Mackman A, Vasireddy S, Dunner M, Escamilla R, Murukan A. Improving we application security: threats and counter measures. Satyam Computer Services, Microsoft Corporation; 2003.
- International Telecommunication Union (ITU), (2014). Measuring the Information Society Report 2014, ISBN 978-92-61-15291-8, Accessed on 08/04/2023, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf
- National Institute of Standards and Technology (NIST), (2018). Cybersecurity Framework Version 1.1. Retrieved from- https://www.nist.gov/publications/cybersecurity-framework-version-11, accessed on 04/04/2023
- Open Web Application Security Project (OWASP), (2017). OWASP Top Ten Project. Accessed on 09/04/2023. Retrieved from- https://owasp.org/Top10/

- Basic definitions and concepts of cyberspace, Ahmed Jamal et al., (2021); Alghamdie, (2021); Bullock et al.,(2021)
- World Bank. (2014). World Development Report 2014, THE WORLD BANK: PROMOTING OPPORTUNIT Y, GROW TH, AND PROSPERIT Y, Oxford: Oxford University Publishers.
- Karim, M. A., & Hasan, R. (2020). Cyber Security Challenges in Bangladesh: An Exploratory Study. Journal of Information Security, 11(3), 168-180
- (Mouna Jouinia,*, Latifa Ben Arfa Rabaia , Anis Ben Aissab, ., (2014) Classification of security threats in information systems, Procedia Computer Science 32 489 – 49 doi: 10.1016/j.procs.2014.05.452
- Shweta Mittal(&) and P. Vigneswara Ilavarasan Department of Management Studies, Indian Institute of Technology, Delhi, India f12shwetam@iima.ac.in, vignes@iitd.ac.in
- Cyber security capacity review, Bangladesh (August 2018)
- Ahn, J., Hwang, J., & Shin, J. (2017). Cybersecurity vulnerabilities and threats in the healthcare sector. Healthcare informatics research, 23(4), 286-293.
- Al-Abdullah, A., & Al-Sayed, A. (2020). Cyber security vulnerabilities in the financial sector. International Journal of Advanced Computer Science and Applications, 11(1), 347-352
- Hossain, M. S., & Rahman, M. R. (2020). Cybersecurity Vulnerabilities and Threats in Bangladesh: A Review of the Literature. Journal of Information Security, 11(3), 155-171
- Ahmed, M., & Hasan, M. R. (2019). Cybersecurity Vulnerabilities in Bangladesh: A Review. International Journal of Cyber Criminology, 13(1), 55-76
- Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI Computer Crime and Security Survey – 2006. 11th Annual CSI/FBI Computer Crime and Security Survey; 2006.
- Woodrow Wilson, (1887), The Study of Administration, Political Science Quarterly, Vol. 2, No. 2, pp. 197-222 . https://doi.org/10.2307/2139277
- Weber, Max. (1947). The Theory of Social and Economic Organization. Translated by A.M. Henderson and Talcott Parsons. London: Collier Macmillan Publishers,

- Cyber security capacity review, Bangladesh –(2018), https://www.researchgate.net/publication/344022535_Cybersecurity_Capacity_Review_Bangladesh
- ISO. Information Processing Systems-Open Systems Interconnection-Basic Reference Model. Part 2: Security Architecture, ISO 7498-2; 1989.
- Farahmand F, Navathe SB, Sharp GP, Enslow PH. A Management Perspective on Risk of Security Threats to Information Systems, Information Technology and Management archive; 2005;6: 202-225.
- United Nations Office on Drugs and Crime (UNODC) (2013), Comprehensive Study on Cybercrime. Accessed on 07/05/2023, Retrieved from – https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_Egmont_2013_study_cybercrime.pdf
- Bangladesh Association of Software and Information Services (BASIS), (2020). Annual Report, 2020. Accessed on 04/04/2023, https://basis.org.bd/annual-report
- Government of Bangladesh Information security Manual (GOBISM), BCC, Feb, 2016
- "ICT Act, 2006 bangladesh," http://bdlaws.minlaw.gov.bd/bangla_pdf_part.php?id=950&vol=37&search=2006/, [Online; accessed 20 April-2023].
- National Institute of Standards and Technology (NIST), (2020). Security and Privacy Controls for Information Systems and Organizations. Special Publication 800-53 Rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Accessed on 05/04/2023.
- ITU, (2014), Cybersecurity. ITU News. Retrieved from https://www.itu.int
- World Economic Forum. 2019. The cyber security guide for leaders in today's digital world. Shaping the future of cyber security and digital trust. World Economic Forum. 1–24.
- Bangladesh Cyber Landscape (2022), https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d_5097_46ba_afa4_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf
- The Information & Communication Technology Act, 2006. (2006). The Information & Communication Technology Act, 2006. 39. Retrieved 02.08.2014 from http://www.prp.org.bd/downloads/ICTAct2006English.pdf

- Sectoral Cyber Threat Intelligence for banking industries (July,2022) https://shop.cirt.gov.bd/product/sectorial-threat-intelligence-for-banks-july-2022/
- Wilson, W. (1941). The study of administration. Political Quarterly, 1941, quoted in Gurmeet Kapoor(1986), Public Administration. Delhi: Macmillan India Limited.
- Weber, M. (1958). Bureaucracy in H. H. Gerth and C. Wright Mills (eds.), in Max Weber, Essays in Sociology. New Jersey: Oxford University Press
- B. Klievink &M. Janssen, (**2009).** Realizing joined-up government — Dynamic capabilities and stage models for transformation, Government Information Quarterly 26(2):275-284. DOI:10.1016/j.giq.2008.12.007
- Parker, A., & Tritter, J. (2006). Focus group method and methodology: Current practice and recent debate. International Journal of Research & Method in Education, 29, 23–37.
- M. A. Khan, A. Salah, and A. Al-Fuqaha (2019). Cybersecurity Vulnerabilities in the Internet of Things (IoT)"; Future Generation Computer Systems. 82: 395-411.
- J. Graham, J. Hieb and J. Naber, "Improving cybersecurity for Industrial Control Systems," *2016 IEEE 25th International Symposium on Industrial Electronics (ISIE)*, Santa Clara, CA, USA, 2016, pp. 618-623, doi: 10.1109/ISIE.2016.7744960.
- The Digital Device, Internet & Information Security Guide Line, Cabinet División (2020)
- Abouzakhar, Nasser & Jones, Andy & Angelopoulou, Olga. (2017). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector, https://ieeexplore.ieee.org/abstract/document/8276780
- Victoria Clarke & Virginia Braun (2017) Thematic analysis, The Journal of Positive Psychology, 12:3, 297-298, DOI: 10.1080/17439760.2016.1262613
- Bangladesh Cyber security strategy, BGD e-GOV CIRT (2021-2025), https://www.cirt.gov.bd/meeting-on-bangladesh-cybersecurity-strategy-2021-2025-responsibility-matrix/

Questionnaire
‘Cyber Security Challenges'

Dear Respondent,

You are requested to fill this questionnaire on the identification of cyber security challenges. The data will be used only for research purpose. It will be highly appreciated if you spend a few minutes from your valuable time to answer the questions. For any query: mashrafulalam@yahoo.com; cell: +8801556304034.

For your convenience, some important terms are defined as follows:
1. Cyber Security: It is the method of safeguarding networks, computer systems, and their components from unauthorized digital access

2. Cyber Threats: It is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches and other attack vectors.

3. Cyber Vulnerabilities: A vulnerability in security refers to a weakness or opportunity in an information system that cybercriminals can exploit and gain unauthorized access to a computer system. Vulnerabilities weaken systems and open the door to malicious attacks.
4. Cyber Attack: When there is an unauthorized system/network access by a third party, it is called a cyber attack.

Thank you very much for your cooperation

Md. Shaiful Islam
Joint Secretary
Team Leader
Research Team

* Required

Part One:

General Information

Please, answer the following questions by clicking in the circle that suits you.

1. Your Gender *
   - Male
   - Female
   - Transgender
2. Your Age
   - 20-30
   - 31-40
   - 41-50
   - 50+
3. Your Educational Degree *
   - Diploma or below

- Bachelor
- Master's degree or higher
- Diploma/Masters on ICT

4. Your Organization's type *
- Ministry
- Division
- Field Office

5. Your are working as personnel of your organization in the *
- ICT cell
- General Employee (Administrative)
- Top Management (Joni Secretary & Above)
- Other

6. How many services of your organization have been digitalized?
- 1-3
- 3-5
- More than 5

Part Two:

Antivirus Software, Anti-Spyware & Firewall etc.

Please, answer the following questions by clicking in the circle that suits you.

1. Who is responsible for installing and maintaining security software on your computer/laptop/server? *
- Employees
- Administrator
- IT Person
- Vendor

2. Does your organization use licensed software and update regularly?*
- Yes
- No
- Do not Know

3. Which operating system is installed on the computers/laptops that you organization normally use to connect to the Internet?*
- Windows 11
- Windows 10
- Windows 8
- Windows Vista
- Windows XP
- Linux
- Other

4. Which web browser do you normally use in your organization? *
- Mozila Firefox
- Microsoft Edge
- Opera
- Netscape
- Google chrome
- Other

5. Are the servers, desktop computers and laptops in your organization using anti-virus software?
- Yes
- No
- Don’t know

6. Which anti-virus software do you use? *
- Paid software
- Free software
- Trial version
- Other

7. Do you update your antivirus software regularlay? *
- Yes
- No

8. Does the organization perform backup and restoration procedures on a regular basis and verify that viruses are not corrupting the backup data? *
- Yes
- No

9. Do your organization use internet security options in computers? *
- Yes
- No
- Other

10. Is Add blocker used in the browser of your organization?*
- Yes
- No

11. Does your organization provide remote access to the servers installed? *
- Yes
- No

Part-3

Software Development/ Vulnerability (vendor related)

1. Are you ensuring security using a firewall in the local area network installed in your organization?*
- Yes
- No
- Donot Know

2. Is the administration (Higher Authority) monitoring your computer all the time? *
- Yes
- No
- Don’t Know

3. Are backup personnel identified and trained for all key positions and critical functions?*

- Yes
- No

4. Are key vendors or service providers required to notify the organization immediately of a known or suspected compromise of customer information? *

- Yes
- No
- Not Applicable

5. Have SSL certificates been used to ensure security in the application software used in your organization? *

- Yes
- No

6. Is the software developed in your organization regularly checked for vulnerability (like VAPT) and SQTC (Software Quality Testing and Certification Centre) test?
*

- Yes
- No
- Donot Know

7. Is software patch updated regularly in your organization? *

- Yes
- No

8. Is Capcha or Two factor authentication method implemented before logging in to the application software used by your organization?*

- Yes
- No

9. Does your organization give vendors access to the network? *

- Yes
- No
- Not Applicable

10. Is the piracy software used in your organization? *

- Yes
- No

11. Does your organization automatically cut off system access once a vendor's engagement is complete? *

- Yes
- No
- Option 3

Part-4

Password Protection

1. Are the computer users in your organization accessing the computer using user ID and password? *
- Yes
- No
- Do not Know

2. Do you use the same password as used in desktop and laptop computers to protect the routers, wireless access points, switches and firewalls in your organization? *
- Yes
- No

3. Is the user password of the used software changed regularly? *
- Yes
- No

4. Is your organization WiFi password (s) shared to strangers (outsider of your org.)?*
- Yes
- No
- Donot know

Part-5

Data Protection

1. Does the organization encrypt its backup data storage devices? *
- Yes
- No
- Not Applicable - there is no backup system

2. Is your organization's software hosted in National Data Center/ BDCCL (Bangladesh Data Centre Company Ltd)? *
- Yes
- No

3. Whether the source code of the developed software, database, required credentials and documentation are obtained from the vendor organization?*
- Yes
- No

4. Is your organization's software developed following BNDA guidelines?*
- Yes
- No

Part-6

Monitoring & Training

1. Does the organization have a process for intrusion detection and are employees trained to monitor intrusion properly? *
- Yes
- No

2. Who looks after the system security owned and managed by your organisation that is not hosted on Data Center?*
- Your organization
- An external provider
- Vendor

3. Do you allow a stranger to use your desktop, laptop or server in your organization?*
- Yes
- No

4. Do you regularly refrain from using pre-proxy sites? *
- Yes
- No

5. Does the top management support the IT team in matters like budgeting, decisions, etc. for system security? *
- Yes
- No

6. Are cyber security awareness and techniques included in the organization's training module?*
- Yes
- No

Part-7

Cyber Attack

1. Have you ever been attacked by clicking on untrusted links?*
- Yes
- No

2. Have you ever experienced a significant cybersecurity incident? Please define and describe it.

3.. What type of attack did you experience in your organization?*
- Denial of Service (DoS)
- RANSOMWARE
- Cyber Bullying
- Phishing and Spear Attacks
- Business Email Compromise
- Malware Attack
- Viruses
- Email/internet Worm
- Adware and Spyware
- Identity Theft/ Private information
- Hacking and predators
- Sexting
- Other

4. Is Government official e-mail used in your organization? *

- Yes
- No

5. Do you open the documents attached to suspicious e-mails?*
   - Yes
   - No

6. Does your organization's firewall allow to download pirated video or other contents ?*
   - Yes
   - No
   - Do not know

7. Do you allow others to use USB to your official laptop/computers/server?*
   - Yes
   - No
   - Sometimes

8. Does Your organization follow Government e-mail policy?*
   - Yes
   - No

9. Have any other steps been taken to ensure cyber security in your organization?
Write down here

Your e-mail no.

Submit