COMMAND AND STAFF TRAINING INSTITUTE
BANGLADESH AIR FORCE

Junior Command and Staff Course

MANAGEMENT MODULE
Information Management
MGT-3

August - 2016

INFORMATION MANAGEMNT

TABLE OF CONTENTS

MGT-3

TOPIC-1

INFORMATION MANAGEMNT

Introduction

1.   **Information management** (**IM**) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This sometimes involves those who have a stake in, or a right to that information. Management means the organization of and control over the structure, processing and delivery of information. In short, information management entails organizing, retrieving, acquiring and maintaining information. It is closely related to and overlapping with the practice of data management.

2.   Improving information management practices is a key focus for many organisations, across both the public and private sectors. This is being driven by a range of factors, including a need to improve the efficiency of business processes, the demands of compliance regulations and the desire to deliver new services. In many cases, 'information management' has meant deploying new technology solutions, such as content or document management systems, data warehousing or portal applications. These projects have a poor track record of success, and most organisations are still struggling to deliver an integrated information management environment. Effective information management is not easy. There are many systems to integrate, a huge range of business needs to meet, and complex organisational (and cultural) issues to address.

Exploring Information Management

3.   'Information management' is an umbrella term that encompasses all the systems and processes within an organisation for the creation and use of corporate information. In terms of technology, information management encompasses systems such as:

    a.   Web content management (CM)

    b.   Document management (DM)

    c.   Records management (RM)

    d.   Digital asset management (DAM)

    e.   Learning management systems (LM)

    f.   Learning content management systems (LCM)

    g.   Collaboration

    h.   Enterprise search

4.   Information management is much more than just technology. Equally importantly, it is about the business processes and practices that underpin the creation and use of information. It is also about the information itself, including the structure of information

1

('information architecture'), metadata, content quality, and more. Information management therefore encompasses:

    a.   People
    b.   Process
    c.   Technology
    d.   Content

Basic Concept

Content Of Human Mind

5.   Good information is required to influence strategic decisions and improve response, but this cannot be gained from the data collected from assessments immediately. Data must first be turned into information, before that can provide knowledge of the current situation and an understanding of the suitable actions to respond. The content of the human mind can be classified into four categories:

    a.   **Data:** symbols

    b.   **Information:** data that are processed to be useful; provides answers to "who", "what", "where", and "when" questions

    c.   **Knowledge:** application of data and information; answers "how" questions

    d.   **Wisdom:** evaluated understanding

Data

6.   **Data** are the raw results from assessments and measurements. Data can be quantitative or qualitative, but quantitative data often concern information managers more. Data, on their own, is often difficult to assimilate, and it is part of the role of an information manager to turn data into usable information.

Information

7.   **Information** is data that have been processed or analyzed in some way, to ensure that the data become meaningful and can assist decision-makers in developing an informed strategy. For example, listing the villages where an organization is present is not all that easy to interpret needs from. Presenting that data as a map, however, can provide constructive information in highlighting which villages are not receiving any assistance.

Knowledge

8.   **Knowledge** is the meaning of information. Knowledge is the combination of the information provided, and background information on similar situations, to interpret the meaning of the information, for example determining what is required in a given situation.

2

Wisdom

9.   **Wisdom/evaluated understanding** is the final stage in the process, and means knowing what action needs to be taken as a result of the knowledge gained about the current situation. It is the understanding that needs to be built into the strategy.

10.   For an example of the transition from data to understanding:

a.   1234 is data.

b.   "There are 1234 refugees in this camp" is information.

c.   "To provide water and sanitation for that many refugees requires at least 62 toilets" is knowledge.

d.   "I'd better procure more material for constructing latrines!" is action.

Info Life Cycle

11.   Information life cycle management (ILM) is a comprehensive approach to managing the flow of an information system's data and associated metadata from creation and initial storage to the time when it becomes obsolete and is deleted. It has the following phases:

a.   Phase 1: Create

b.   Phase 2: Store

c.   Phase 3: Use

d.   Phase 4: Share

e.   Phase 5: Archive

f.   Phase 6: Destroy

Phase 1: Create

12.   During the first phase, structured or unstructured data is created. It can be in the form of an MS Office 365 document, a PDF file, email, information in a database, or even images. Often in this phase, security classification occurs based on an enterprise data security policy.

Phase 2: Store

13.   Once a file is created, it is stored somewhere. At this point, you need to ensure that stored data is protected and the necessary data security controls have been implemented.

Phase 3: Use

14.   Once a file is created, it is stored and then used. During this stage, data is viewed, processed, modified and saved. Here, security controls are applied to data at point of

use. You need to be able to monitor user activity and apply security controls to ensure data leak prevention.

Phase 4: Share

15.   Data is constantly being shared between employees, customers and partners, necessitating a strategy that continuously monitors data stores for new instances of sensitive data. Data moves among a variety of public and private storage locations, applications and operating environments, and is accessed by various data owners from different devices and platforms. That can happen at any stage of the data security lifecycle, which is why it's important to apply the right security controls at the right time.

Phase 5: Archive

16.   At some point, data may leave active use and get archived. Once archived, it's important that the data be both available and protected.

Phase 6: Destroy

17.   The volume of archived data inevitably grows, and while you may want to save all your data forever, that's not feasible. Cost and compliance issues exert pressure to destroy data you no longer need.

The Information Management Continuum

18.   The principle goal of the information management function is to provide clear information products to the field that can guide decision makers. These products may in the form of tables, maps or reports, or may form part of other documents. An information management system will be successful if it begins with determining what information is needed, then collects and analyses that information and finally presents it in a way which allows decisions to be made, which is simply diagrammed as:
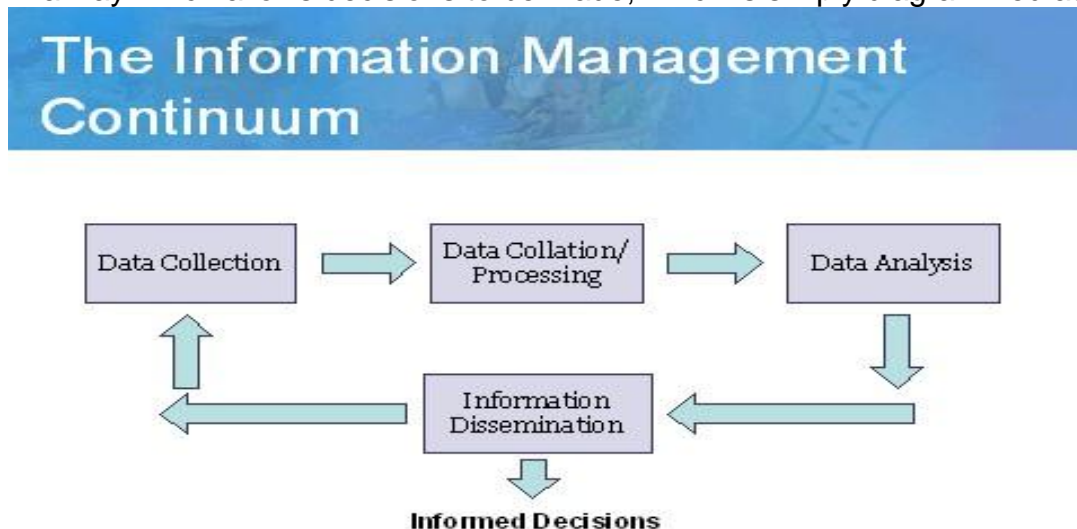
a.   Data Collection.   The process of gathering assorted, relevant datasets from various sources such as local government, other clusters, UN/OCHA and other UN Agencies, and operational agencies that are active in the cluster.

4

b. <u>Data Collation.</u> The process of putting together the various datasets into a format that can be stored, accessed and easily analysed.

c. <u>Data Analysis.</u> The strategic combining of the various datasets into meaningful information that can be used by decision makers in the cluster.

d. <u>Information Dissemination.</u> An important process of ensuring that the various analyses and information that is generated are made available to relevant stakeholders In the most appropriate way.

Principles of Information Management

19. There are ten key principles to ensure that information management activities are effective and successful:

a. Recognise (and manage) complexity

b. Focus on adoption

c. Deliver tangible & visible benefits

d. Prioritise according to business needs

e. Take a journey of a thousand steps

f. Provide strong leadership

g. Mitigate risks

h. Communicate extensively

j. Aim to deliver a seamless user experience

k. Choose the first project very carefully

Principle 1: Recognise (and manage) complexity

20. There are no simple answers. The complexity is difficult to avoid. There are no 'silver bullet' solutions. It requires strong leadership to set a clear direction, and many incremental improvements.

Principle 2: Focus on adoption

21. Systems without users are useless. Carefully structure your projects to focus on user adoption from the onset. Ensure there are enough people using the systems to make them valuable.

Principle 3: Deliver Tangible & Visible Benefits

22. Creating a common data definition or taxonomy is great for efficient information management. However, very few users will ever notice these improvements. On the

5

other hand, providing timely, reliable, and accurate operational management information will. Wrap back-end improvements into these.

Principle 4: Prioritise According to Business Needs

23.   Base the planning process on ability to address business needs. Keep the overall technology strategy Creating a common data definition or taxonomy is great for efficient information management. However, very few users will ever notice these improvements. On the other hand, providing timely, reliable, and accurate operational management information will. Wrap back-end improvements into these.

Principle 5: Take a Journey of a Thousand Steps

24.   Let go of the desire to create a perfect plan. The problem is too complex. 'Analysis paralyses' waits if you search for the perfect solution. Big improvements are achievable by implementing hundred, or even thousands, of small co-ordinated changes across the company.

Principle 6: Provide Strong Leadership

25.   Decide how the business will operate, including the information needed. Develop this vision and communicate it clearly.

Principle 7: Mitigate Risks

26.   Apply good risk management to ensure success. Identify risks and define the approach to minimise their potential impact.

Principle 8: Communicate Extensively

27.   Make sure everyone knows the business direction and desired outcomes. Remind them often. This way each business unit can make the best decisions to support the goal.

Principle 9: Aim to Deliver a User Experience

28.   Users do not care about which system data came from. A seamless user experience hides the systems information is coming from. You do not need one large system, but aim for the users accessing whatever they need from one place.

Principle 10: Choose the First Project Very Carefully

29.   The first project is the best (and possibly last) opportunity to prove the value of information management. Select a manageable project, with visible benefits; in an area of the business, everyone has an interest.

Information Management Challenges

30.   Organisations are confronted with many information management problems and issues. In many ways, the growth of electronic information (rather than paper) has only

worsened these issues over the last decade or two. Common information management problems include:

   a.   Large number of disparate information management systems.

   b.   Little integration or coordination between information systems.

   c.   Range of legacy systems requiring upgrading or replacement.

   d.   Direct competition between information management systems.

   e.   No clear strategic direction for the overall technology environment.

   f.   Limited and patchy adoption of existing information systems by staff.

   g.   Poor quality of information, including lack of consistency, duplication, and out-of-date information.

   h.   Little recognition and support of information management by senior management.

   j.   Limited resources for deploying, managing or improving information systems.

   k.   Lack of enterprise-wide definitions for information types and values (no corporate-wide taxonomy).

   l.   Large number of diverse business needs and issues to be addressed.

   m.   Lack of clarity around broader organisational strategies and directions.

   n.   Difficulties in changing working practices and processes of staff.

   p.   Internal politics impacting on the ability to coordinate activities enterprise-wide.

While this can be an overwhelming list, there are practical ways of delivering solutions that work within these limitations and issues.

Conclusion

31.   Implementing information technology solutions in a complex and ever-changing organisational environment is never easy. The challenges inherent in information management projects mean that new approaches need to be taken, if they are to succeed. Step-by-step approach to implementing solutions that starts with addressing key needs and building support for further initiatives. A focus on adoption then ensures that staff actually use the solutions that are deployed. Of course, much more can be written on how to tackle information management projects. Future articles will further explore this topic, providing additional guidance and outlining concrete approaches that can be taken.

TOPIC-2

COMPUTER NETWORKING (LAN, WAN AND BAF NETWORKING SYSTEM)

Introduction

1.   Suddenly it seems that the networking is everywhere. The explosive growth of the networking is a revolutionary phenomenon in computing and telecommunication. The LAN/WAN has become the largest and most important network of today's network and has evolved into a global information superhighway. The LAN/WAN is constantly expanding more and more for businesses and other organization and their users, computers and networks join its global web. The LAN/WAN has also become a key platform for a rapidly expanding information and entertainment services. Merely having a transmission pathway does not produce communication. When two entities communicate, they do not merely exchange data; rather, they understand the data they receive from each other. The goal of computer networking, therefore, is not simply to exchange data, but to be able to understand and use data receive from other entities on the network.

What is Network

2.   A Network is a set of devices (often referred to as nodes) connected by media links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. The links connecting the devices are often called communication channels. A network is a group of inter connected system sharing services and inter tracing by shared inter tracing line. A network, therefore, requires two or more individual systems with something to share (data). The individual system must be connected through a physical pathway (Called the transmission medium). All systems on the physical pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules that govern Computer communication are called protocols.

3.   In summary, all networks must have the following:

    a.   Some thing to share (data).

    b.   A physical pathway (transmission media).

    c.   Rules of communication (protocols).

Categories of Networks

4.   Today when we speak of networks, we are generally referring to three primary categories: local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). Which category a network falls into is determined by its size, its ownership, the distance it covers, and its physical architecture.

    a.   **Local Area Network (LAN).**   LAN is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs

and a printer in someone's home office, or it can extend throughout a company and include voice, sound, and video peripherals. Currently, LAN size is limited to a few kilometers.

    b.   **Metropolitan Area Network (MAN).**   MAN is designed to extend over an entire city. It may be a single network such as a cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device. MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company, such as a local telephone company.

    c.   **Wide Area Network (WAN).** WAN provides long distance transmission of information over large geographical areas that may comprise a country, a continent, or even the whole world.

BAF Networking System

5.   The backbone of the existing LAN/WAN is connected through BAF digital LOS microwave sys. At times, due to unsvc/malfunctioning of the microwave sys, the online op with central server from different Bases/Units gets interrupted. For seamless connectivity, optical fiber link is also installed as an alternate to the existing BAF owned LOS link. Let us have a look of present IT infrastructure in BAF.

    a.   BAF has been establishment of world class Computer Network for all BAF premises, BAF possesses its own LAN/WAN network covering almost all the bases and units. The network is a hybrid one comprising optical fiber and MW backbone.

    b.   BAF established its own Data Center which contains state of the earth servers, storage devices, network devices, DR server loc at diff place and related safety requirements.

    c.   Approx Workstation 601 which is increasing day by day.

    d.   This BAF network is using for

        (1)   BAF Customized Software

        (2)   Official mailing system and

        (3)   BAF Web site

6.   We can access these available facilities from different BAF bases. Users from these BAF bases are connected through LAN/WAN & Microwave. At present the total no of users is 601. Among these users:

    a.   Air HQ has 140 users which is connected with optical fibre.

    b.   Base BBD has 120 users which is connected with optical fibre & microwave.

c.   Base ZHR has 106 users which is connected with optical fibre & microwave.

d.   Base BSR has- 82 users which is connected with optical fibre.

e.   Base MTR has- 113 users which is connected with optical fibre & microwave.

f.   Base PKP has- 35 users which is connected with microwave.

TOPIC-3

BAF CUSTOMIZED SOFTWARE

Introduction

1.   Project for development of Customized Software for BAF was under taken in the year of 2001. Through the tender process, a local software company was selected to develop the Customized Software for BAF. The project for development of Integrated Customized Software started in Feb 05. The Vendor's Developer Team developed the modules/sub-modules for all potential users of BAF as per BAF reqr under the supervision of BAF Task Party. The development phase of the project was completed on 31 May 07. As a part of the implementation plan, the Vendor's Developer Team and BAF Task Party arranged training for BAF personnel (Operators & Database Administrators (DBA) of different Bases and Units for smooth technology transfer among BAF personnel. The Task Party also visited different Bases/Units to provide necessary guidelines to the users for smooth use of the customized software. On **06 Nov 07,** the BAF Integrated Customized Software was put into operation and declared open to all users of BAF.

Objectives

2.   The objective of developing the BAF Customized software are:

    a.   Quick retrieval, dissemination and sharing of data/info.   By   using Customized software, different sections can easily and quickly retrieve, disseminate and share data/information irrespective of their location through common network.

    b.   Instantaneous report generation to assist planning and decision making process.   By using Customized software, personnel instantly gets reports, which are useful in planning; As such immediate decisions can be made. Consequently Operations, Maintenance, Administration and Training activities Management are done efficiently.

    c.   Efficient Logistic and Financial planning, monitoring and control.   When information is updated in the central network, user's can- plan, monitor and control logistic and financial matters more effectively.

    d.   Effective utilization of Human and other Resources.   One of the major benefits of Customized software is that it exploits available resources effectively.

    e.   Saves Time and Money.   For example, when mails are dispatched through the mailing system, the user does not have to send it by hand, which saves time and money and reduces office and other overhead expenditures.

    f.   Reduces human error and mistakes.   If data input is given to the computers, then processing of data will be done without any mistake or human error.

11

g. <u>Enables quick and timely decision making.</u> IT enables in making uninterrupted communication between users of different bases. Therefore the decision makers can receive valuable information in time and can give decisions quickly.

List Of All Modules

4. A total of 38 modules/sub modules have been developed based on the OPI Dte/concerned users requirement. The modules are as under:

S/No	Name of Module
1.	Personnel Management Information Sys
2.	Flying Information Sys
3.	Aircraft Maintenance Information Sys
4.	Air Defense Information Sys
5.	Finance and Accounting Information Sys
	Officer Pay Role System(FCIS)
6.	Demand and Supply Information Sys (DSIS)
7.	Stock and Inventory Management Sys
8.	Catering Information Sys
9.	Flight Safety Information Sys
10.	Meteorological Information Sys
11.	Air Traffic Control Information Sys
12.	Accommodation Information Sys
13.	Medical Information Sys
14.	Library Management Information Sys
15.	Mess Accounting Information Sys
16.	Ops Room Information Sys
17.	Mechanical Transport Information Sys
18.	Air Training Information Sys
19.	Inspection Information Sys

20.	AFI / AFO Archive
21.	RCN Exchange Information
22.	PDO Archive
23.	Planning Information Sys
24.	Budget Information Sys
25.	Central Quality Control(CQC)
26.	Legal Information Sys
27.	Intelligence Information Sys
28.	Security Management Information Sys
29.	Works Information Sys (Project)
30.	Recruitment Management Information Sys
31.	Press Management Information Sys
32.	Pension & Provident Fund Information Sys
33.	Communication Information Sys
34.	Training Institute Information Sys
35.	205 MU Information Sys
36.	212 MU Information Sys
37.	Armament Information Sys (Eqpt Inventory)
38	School of Security and Intelligence Info Sys

Modules In Operation

4.   At present 08 out of 38 modules are being used by different users. List of the modules in use are as follows:

S/No	Name of Module
1.	Personnel Management Information Sys
2.	Catering Information Sys
3.	Aircraft Maintenance Information Sys

13

RESTRICTED

4.	Finance and Accounting Information Sys
5.	Meteorological Information Sys
6.	Library Management Information Sys
7.	AFI / AFO Archive
8.	Communication Information Sys

Requirements For Implementation

5.   In order to ensure smooth implementation of the BAF Customized Software, the following Requirements may be taken into consideration at the earliest:

a.   More Users Involvement/support

b.   Maintain smooth and uninterrupted Connectivity of Fiber Optic Link and Microwave Link for BAF LAN/WAN

c.   Up-gradation of BAF LAN/WAN network

d.   Dedicated PC for all Users

e.   Regular Cleaning of virus using appropriate Ant-Virus

f.   Regular data Entry by Users of each Module/Sub-Module

g.   Dedicated System Support Team and Training

h.   Ensure compliance of SOPs and Directives

i.   Monitoring by Directorates

j.   Base Wise 'Local Implementation Committee

k.   Maintaining Liaison with Central Server for Support

l.   Continuous updating of Users Requirements

m. Maintain Security of Information

Conclusion

6.   The development and up-gradation of the BAF Customized software is a continuous process, which largely depends on the users' interaction with the system and giving feedback to the Project Office. Proper awareness for utilization of the system and official directives and instructions are required for ensuring the use of the system at all levels. A Core Group of Officers assisted by a 'Implementation Team' and supervision by Directorates are of prime importance to ensure the effective maintenance and use of the system. Side by side, the enhancement of the connectivity, procurement of Hardware is also required. The success of the project implementation is a combined effort at all levels of BAF. Maximum output of Utilization of IT system depends on the computer literacy of BAF personnel.

TOPIC-4

CYBER CRIME AND SECURITY

Introduction

1.   With the development of science and technology, life has become comfortable and faster; specially the recent development in ICT field has made a remarkable change in the life-style. Now a day, physical movement has become a rare issue to do anything like taking the service, paying the bills, e-ticketing, e-banking and e-governance etc. However, the other part of this ICT world has a darker side which may be compared with the unethical use of nuclear energy – like a nuclear bomb. As more and more people are getting used to run with cyber world, the mis-use of it can also cripple the like-cycle. Cybercrimes are created with the help of the internet for internet banking fraud, botnets, computer intrusion or hacking and specially the distributed denial of service (DDOS) attacks. Traditional crimes helped by the internet includes frauds and scams, money laundering, drug trafficking, terrorism, child sexual exploitation and so on.

2.   Cybercrime knows no boundary whereas; the law enforcing agencies cannot cross the border. More so this is quite a dangerous issue because the cyber criminals are highly educated and they are smarter than the personnel of law enforcing agencies. Rapid growth of mobile and wi-fi devices has added a greater risk to deal with this issue. It is other-way good news that we have not become dependant on cybernet like the first world countries to be affected by cybercrime in greater scale. However, it is high time for us to be prepared and get sensitized to fight with cybercrime and criminals.

Definition of Cyberspace and Cybercrime

3.   **Cyberspace.** An electronic medium of computer system within which people can communicate do research, or simply window shop.

4.   **Cybercrime.** Cyber crime—also known as computer crime, e-crime and electronic crime. Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs is called cybercrime. Cybercrime is nothing but where the computer used as an object or subject of crime.

History Of Cybercrime

5.   The *first recorded cybercrime* took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C.

6.   The first spam email took place in 1978 when it was sent out over the Arpanet (Advanced Research Projects Agency Network).

7.   The first virus was installed on an Apple computer in 1982 when high school student, Rich Skrenta, developed the Elk cloner.

Categories of Cybercrime

8.   We can categorize cybercrimes in two ways:

a.   **The Computer as a Target**: - Using a computer to attack other computers. e.g. hacking, virus/worm attacks, DoS attack etc where computer is used as a target.

b.   **The computer as a weapon:** - Using a computer to commit real world crimes. e.g. cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc where computer is used as a weapon.

Types Of Cyber Crimes

9.   There are several types of Cybercrime, some of the common forms are:

a.   **Hacking**.   It is an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Most hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

b.   **Phishing.**   The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

c.   **Child Pornography**.

(1)   The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide.

(2)   Its explosion has made the children a viable victim to the cyber crime.

(3)   As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of pedophiles.

d.   **Internet Fraud.**   The term Internet fraud refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme.

e.   **Cyber Stalking**.   Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services,(such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects).

f.   **Virus Dissemination**.   Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the examples of malicious software)

g.   **Software Piracy**.   Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

h.   **Credit Card Fraud**. The unauthorized and illegal use of a credit card to purchase property.

j.   **Net Extortion**. Copying the company's confidential data in order to extort said company for huge amount

k.   **Trojan**. It is a malicious program that is disguised as or embedded within legitimate software. A trojan is designed to operate with functions unknown to the victim.

l.   **Denial of Service (DoS) Attack.** This is an act by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with spars mail depriving him of the services he is entitled to access or provide, Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

m.   **Computer Vandalism.**   Damaging or destroying data rather than stealing or misusing them is called cyber vandalism.

n.   **Transmitting virus.** These are programs that attach themselves to a file and then circulate. They usually affect the date on a computer, either by altering or deleting It against properties.

p.   **Cyber Terrorism.**   Terrorist attacks on the Internet by distributed denial of service attacks, hats websites and hate emails, attacks on sensitive computer networks, etc.

q.   **Botnet**.
        (1)   Exploits large numbers of Internet connected computers.
        (2)   Some of the uses of botnets include sending out spam e-mails, launching   distributed denial of service attacks (DDoS) and host fraudulent web sites (such as false bank websites).

17
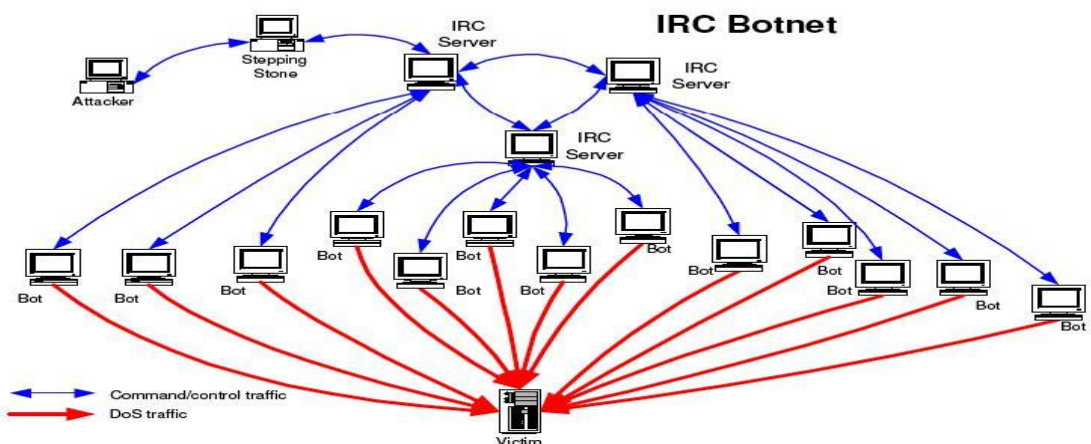
Present Trends of Cybercrime in Bangladesh

10.   Few present trends of cybercrime in Bangladesh are highlighted below:

      a.   Malicious mail to foreign diplomatic mission and other VIPs.
      b.   Pornography.
      c.   Use of e-mail for illegal activities.
      d.   Use of internet for transmitting false and malicious information.
      e.   Use of internet for prostitution.
      f.   Use of internet for women & child trafficking.

Cyber Security

11.   Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. It involves protection of sensitive personal and business information through prevention, detection, and response to different online attacks.

12.   Cyber security actually protects our personal information by responding, detecting and preventing the attacks.

Cyber Crime Prevention Tips

13.   **Privacy policy.**   Before submitting our name, email address, or other personal information on a website, look for the site's privacy policy. Evidence that our information is being encrypted: To protect attackers from hijacking our information, any personal information submitted online should be encrypted. Many sites use SSL or secure sockets layer to encrypt information for protecting our privacy.

14.   **Keep Software up to Date.**   If the seller releases patches for the software operating our device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage.

15.   **Disable Remote Connectivity.**   Same *PDA's* and phones are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. We should disable these features when they are not in use.

16.   **Use Strong Passwords.**   Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

17.   **<u>Secure Our Computer.</u>**   Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

18.   **<u>Use anti-virus/malware software.</u>**   Prevent viruses from infecting our computer by installing and regularly updating anti-virus software.

19.   **<u>Block spyware attacks.</u>**   Prevent spyware from infiltrating our computer by installing and updating anti-spyware software.

20.   **<u>Be Social-Media Savvy.</u>**   Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check our security settings. Be careful what information we post online. Once it is on the Internet, it is there forever.

21.   **<u>Secure Our Mobile Devices.</u>**   Be aware that our mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

22.   **<u>Install the latest operating system updates.</u>** Keep   our   applications   and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

23.   **<u>Protect Our Data.</u>**   Use encryption for our most sensitive files such as tax returns or financial records, make regular back-ups of all our important data, and store it in another location.

24.   **<u>Secure Our wireless network.</u>**   Wi-Fi (wireless)   networks   at   home   are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

25.   **<u>Protect Our e-Identity.</u>**   Be cautious when giving out personal information such as our name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that we've enabled privacy settings (e.g. when accessing/using social networking sites).

26.   **<u>Avoid being scammed.</u>**   Always think before we click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask we to verify your information or confirm your user ID or password.

27.   **<u>Call the right person for help.</u>**   Don't panic! If we are a victim, if we encounter illegal Internet content (e.g. child exploitation) or if we suspect a computer crime, identity theft or a commercial scam, report this to our local police. If we need help with maintenance or software installation on our computer, consult with our service provider or a certified computer technician.

Acts & Policies By Govt To Prevent Cybercrime

28.   Cyber Law deals with the legal issues of the Cybercrime. There are not enough laws in Bangladesh which may punish the cyber criminals. Bangladesh has enacted the following acts and policies to prevent Cybercrime:

      a.   ICT Act, 2006 (Amdt 2009 & 2013)

      b.   The Right to Information Act, 2009

      c.   Info Sy Policy Guideline, 2014

      d.   Cyber Sy Guideline, 2014

      e.   National Cyber Sy Strategy, 2014

Service Policies

29.   Besides the Govt acts and policies, the service headquarters also have the joint service policies & guidelines. These are:

      a.   Armed Forces Policy Guideline on Social Media and Electronic Gadgets

      b.   Joint Communication and IT Policies

BAF Policies & Guidelines

30.   BAF also has some policies and guidelines on the following issues:

      a.   ICT Policy

      b.   Email Guideline

      c.   Internet Policy

      d.   Information Security Policy

      e.   Social Media and Electronic Gadgets Policy

Facilities of ICT Act:

31.   It provides the following facilities

      a.   It eliminates barriers to e-commerce.

      b.   It promotes legal and business infrastructures to secure e-transactions.

      c.   It facilitates electronic filing in government agencies.

      d.   It ensures efficient delivery of electronic records from government offices

e.   It helps in maintaining the latest technology by freeing it from nuisance as punitive provisions publishing obscene or defamatory information in electronic form.

32.   **Penalty.**   The ICT Act 2006 (Amdt 2009 & 2013) ensures one year to ten years imprisonment and a fine from one lac to one crore taka or both for various offences.

Conclusion

33.   Bangladesh is yet to experience the dangers of cybercrime. The rapid growth of ICT field in our country indicates that the days are not far ahead when our people will start depending on e-banking, e- shopping, e-servicing, e-governance and so on. If we fail to take appropriate measures well ahead to deal with cybercrime, then, our country may be affected by cyber attack like a country named Estonia, which was totally denied from all e-services in 2007. Modern countries have gone far ahead to deal with cybercrime and they are conducting "Cyber Storm Exercises" in regular interval which we have never imagined or never heard of. Again, cybercrime can not be fought alone; it demands the cooperation, support from user and also from other countries. So we have to sensitize about this issue at all level.

TOPIC-5

CLOUD COMPUTING: THE NEW FRONTIER OF INTERNET COMPUTING

Introduction

1.   The Internet, also called the Net, is a worldwide collection of networks that links millions of businesses, government agencies, educational institutions, and individuals. Cloud computing is an Internet service that provides computing needs to computer users. When the company uses the computing resources, they pay a fee based on the amount of computing time and other resources that they consume.

2.   Cloud computing is an emerging technology that has become one of the most popular computing technologies. What is the cloud? Where is the cloud? Are we in the cloud now? These are few very common questions we have probably heard or even asked ourselves. The term "cloud computing" is everywhere. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications.

Internet

3.   One of the major reasons business, home, and other users purchase computers is for Internet access. The Internet, also called the Net, is a worldwide collection of networks that links millions of businesses, government agencies, educational institutions, and individuals. The Internet is a widely used research tool, providing society with access to global information and instant communications.

4.   Today, more than one billion home and business users around the world access a variety of services on the Internet. The World Wide Web, or simply the Web, and e-mail are two of the more widely used Internet services. Other services include chat rooms, instant messaging, and VoIP (Voice over Internet Protocol).

5.   The Internet consists of many local, regional, national, and international networks. Both public and private organizations own networks on the Internet. These networks, along with telephone companies, cable and satellite companies, and the government, all contribute toward the internal structure of the Internet.

6.   Each organization on the Internet is responsible only for maintaining its own network. No single person, company, institution, or government agency controls or owns the Internet. The World Wide Web Consortium (W3C), however, oversees research and sets standards and guidelines for many areas of the Internet. More than 350 organizations from around the world are members of the W3C.

Definition of Internet Computing

7.   Internet computing is the foundation on which e-business runs. It is the only architecture that can run all facets of business, from supplier collaboration and merchandise purchasing, to distribution and store operations, to customer sales and service. Internet computing is the only architecture that supports all information flows and

processes over the Internet — providing access to all applications. With Internet computing, all a user needs is a standard Web browser and security clearance.

8.   Internet computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Internet model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Definition of Cloud Computing

9.   The cloud represents the Internet-based computing resources and the accessibility is through some secure support of connectivity. In the simplest terms, cloud computing means storing and accessing data and programs over the Internet from a remote location or computer instead of our computer's hard drive. This remote location has several properties such as scalability, elasticity etc, which is significantly different from a simple remote machine.

10.   The formal definition of cloud computing comes from the National Institute of Standards and Technology (NIST): "Cloud computing is a model for enabling ubiquitous (global/universal), convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Characteristic Features

11.   Cloud computing has five essential characteristics. If any of these characteristics is missing, then it is not cloud computing:

    a.   **On-demand Self-service**. A user can independently choose computing capabilities, such as server time and network storage, without requiring human interaction with any service provider.

    b.   **Broad Network Access**. Capabilities are available over the network and accessed by wide range of client platforms (e.g., mobile phones, laptops, desktops etc).

    c.   **Elastic Resource Pooling**. The provider's computing resources are pooled to serve multiple users with different physical and virtual resources dynamically assigned and reassigned according to user demand. Users generally have no control or knowledge over the exact location of the provided resources.

    d.   **Rapid Elasticity**. Capabilities can be rapidly and elastically provided to quickly scale out and released to quickly scale in. To the user, the capabilities available appear to be unlimited and can be purchased in any quantity at any time.

    e.   **Measured Service**. Cloud systems automatically control and optimize resource use by utilizing a metering capability. Resource usage can be monitored,

controlled, and reported providing transparency for both the provider and user of the utilized service.

Deployment Models

12. Deployment models describe the ways with which the cloud services can be deployed or made available to its users, depending on the organizational structure and the location. Four deployment models are usually distinguished, namely, public, private, community, and hybrid cloud service usage:

a. **Private Cloud**: The cloud infrastructure is provided for exclusive use by a single organization comprising multiple users (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

b. **Public Cloud**. The cloud infrastructure is provided for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

c. **Community Cloud**. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

d. **Hybrid Cloud**. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Service Offering Models

13. There are three kinds of services with which the cloud-based computing resources are available to end users: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It is also known as the service–platform–infrastructure (SPI) model of the cloud.

a. **Cloud SaaS**: In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The user does not manage or control the underlying cloud infrastructure, with some exception of limited user-specific application configuration settings. Examples: Web-based Email (Gmail, Yahoo etc), Dropbox etc.

b. **Cloud PaaS**: In Platform as a Service model, an operating system, hardware, and network are provided, and the user installs or develops its own software and applications. The user does not manage or control the underlying cloud infrastructure but has control over the deployed applications and possibly

configuration settings for the application-hosting environment. The service provider provides the networks, servers, and storage and manages the levels of scalability and maintenance. Examples: Web Hosting Services, Google App Engine and Microsoft Azure Services etc.

c.   **Cloud IaaS**: The Infrastructure as a Service model provides just the hardware and network; the user installs or develops its own operating systems, software and applications. The user does not manage or control the underlying cloud hardware infrastructure but has control over the operating systems, storage, and deployed applications. The service provider owns the equipment and is only responsible for housing, cooling operation, and maintenance etc. Example: Amazon Web Services (AWS)

Cloud Application

14.   A cloud application is an application program that functions or executes in the cloud; the application can exhibit some characteristics of a pure desktop application and some characteristics of a pure web-based application. A desktop application resides entirely on a single device at the user's location and on the other hand, a web application is stored entirely on a remote server and is delivered over the Internet through a browser interface.

15.   Like desktop applications, cloud applications can provide fast responsiveness and can work offline. Like web applications, cloud applications need not permanently reside on the local device, but they can be easily updated online. Cloud applications are, therefore, under the user's constant control, yet they need not always consume storage space on the user's computer or communications device. Cloud application offers all the interactivity of a desktop application along with the portability of a web application.

16.   An example of cloud application is a web-based e-mail (e.g., Gmail, Yahoo mail); in this application, the user of the e-mail uses the cloud—all of the emails in their inbox are stored on servers at remote locations at the e-mail service provider. However, there are many other services that use the cloud in different ways. Here is yet another example: Dropbox is a cloud storage service that lets us easily store and share files with other people and access files from a mobile device as well.

Advantages

17.   Benefits of cloud computing can be as follows:

a.   **Improved Accessibility**. Data and applications can be accessed anytime, anywhere, using any smart computing device, making our life so much easier.

b.   **Reduced Capital Costs**. There is no need to spend huge money on hardware, software, or licensing fees. It also relieves us from the responsibility and costs of maintenance of the entire computing infrastructure and pushes all these to the cloud vendor or provider.

c.   **Scalability**. Cloud computing also enables precisely the right amount of computing power and resources to be used for applications. Users can draw and

make use as much or as little computing power as they need, being charged only for the usage time/computing power; accordingly, this scheme can save money.

d.   **Minimize Maintenance Cost**. It also relieves us from the responsibility and costs of maintenance of the entire computing infrastructure, including software licensing costs and pushes all these to the cloud vendor or provider.

e.   **Globalize the Workforce**. People worldwide can access the cloud with Internet connection.

f.   **Less personnel Training**. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.

g.   **Improved Flexibility**. It is possible to make fast changes in our work environment without serious issues at stake.

h.   **Reliability**. The cloud also offers a new level of reliability. The virtualization technology enables a vendor's cloud software to automatically move data from a piece of hardware that goes bad or is pulled offline to a section of the system or hardware that is functioning or operational. Separate backup systems, with cloud disaster recovery strategies, provide another layer of dependability and reliability.

j.   **Green Computing**. Cloud computing can reduce the environmental impact of building, shipping, housing, and ultimately destroying (or recycling) computer equipment as no one is going to own many such systems in their premises and managing the offices with fewer computers that consume less energy comparatively.

Drawbacks

18.   Drawbacks to cloud computing are obvious.

a.   If we lose our Internet connection, we have lost the link to the cloud and thereby to the data and applications.

b.   There is also a concern about security as our entire working with data and applications depend on other's (cloud vendor or providers) computing power.

c.   Also, while cloud computing supports scalability (i.e., quickly scaling up and down computing resources depending on the need), it does not permit the control on these resources as these are not owned by the user.

d.   Depending on the cloud vendor or provider, users may face restrictions on the availability of applications, operating systems, and infrastructure options.

e.   And, sometimes, all development platforms may not be available in the cloud due to the fact that the cloud vendor may not aware of such solutions.

f.   A major barrier to cloud computing is the inter-operability of applications, which is the ability of two or more applications that are required to support a business need to work together by sharing data and other business-related

26

resources. Normally, this does not happen in the cloud as these applications may not be available with a single cloud vendor and two different vendors having these applications do not cooperate with each other.

Cloud Computing & BAF

19.   We may find the following from BAF perspective:

a.   Public Clouds would not be suitable for any military organization, as application and data would be stored in providers' location.

b.   Private Cloud software can be utilized, depending on robust network connectivity.

c.   However, Community Cloud or Hybrid Cloud (Community & Private) solutions can be explored while implementing Net-Centric Operations in Joint Service environment.

d.   Application and data, not sensitive in nature, can be stored in public clouds. Example: Mess Accounting Software for all messes.

20.   Advantages of Mess Accounting Software hosted in the cloud:

a.   Less Cost, software is developed & installed in one location, same software can be utilized by all messes.

b.   Hardware resources can be expanded as and when required.

c.   No hardware cost.

d.   Technical & maintenance support provided by cloud service provider.

e.   Easy Connectivity, multiple ways to connect to Internet, i.e. Broadband, 3G etc.

Conclusion

21.   Cloud computing is one of the most popular technologies that has become an integral part of the computing world nowadays. It has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. The usage and popularity of cloud computing is increasing every day and is expected to increase further.