# Information Security in BRAC University: Present and Future


**Prepared by:**

Md. Fahmid Wasif

ID 14164080

BRAC Business School

BRAC University

**Date: September 20, 2016**

# Letter of Transmittal

To

Dr. Salehuddin Ahmed

Professor

BRAC Business School

BRAC University

66, Mohakhali

Dhaka-1212

Subject: Submission of Internship final report

Dear Sir,

This is my great pleasure to submit the internship report of my three months long Internship program in one of the reputed Education Institute 'BRAC University" as a part of the requirement of the course. The title of the report is "Information Security in BRAC University: Present and Future''.

I have put my best effort to make this report a successful one. It has been joyful and enlightening experience for me to work in the organization and prepare this report. However this has been obviously a great source of learning for me.

I would like to express my sincere gratitude to you for your kind guidance and suggestions in preparing the report. It would my immense pleasure if you find this report useful and informative to have an apparent perspective on the issue. I shall be happy to provide any further explanation regarding this report if you have any query on this report or any other relevant matters.

Thanking you in anticipation.

Yours Sincerely,

_____

Md. Fahmid Wasif

ID: 14164080

# Acknowledgement

The success of this Internship report is for the involvement of number of people without whom it would have been tough enough for me to accomplish. It is difficult for me to thank all those people who have some contribution in this report. But there are some special people those are must to be mentioned.

First of all, I would like to thank my honorable academic supervisor Dr. Salehuddin Ahmed, Professor, BRAC Business School, BRAC University. I am thankful to him for his continuous support, supervision and suggestion and giving me valuable information that was very much needed for me to complete this report.

Then, I express my sincere gratitude to BRAC University IT System team for their sincere support.

But, I would like to thank specially my internship Supervisor Mohammad Aminul Islam, Manager GLDN and IT, BRAC University, without whom I would not have been able to learn how an IT department works on which I was able to do my report. I was also constantly supported by the IT team who taught me different aspects of the department. I am highly grateful to all the people who made this report possible.

Lastly, I would like to say that from this internship program I believe the experience that is gathered will definitely help me in the future.

# Executive Summary

Academic institutions face a barrage of information security incidents such as data theft, malicious software infections, hacks into their computer systems, and infiltration of other entities via their networks. Adverse impacts of these incidents include compromised private data and intellectual property, substantial financial losses, and potential threats to critical infrastructure, public safety, and national security. Despite these issues, little research has been conducted at the policy, practice, or theoretical levels, and few policies and cost-effective controls have been developed.

The purpose of the study was to identify security vulnerability and threats, then find some countermeasure to mitigate these vulnerability and threats.

# Table of Contents


Organization ..... 2
Mission ..... 2
Goal ..... 2
Organizational Structure ..... 2
Programs ..... 3
Institutes and Schools ..... 4
Departments ..... 8
Centre and Initiatives ..... 10
Information Security ..... 12
Threats to security ..... 12
Vulnerabilities ..... 12
Threats ..... 14
Malicious Programs ..... 15
Countermeasure ..... 18
Firewalls ..... 18
Antivirus ..... 18
Cyber Attack Globally ..... 19
Information Security in BRAC University ..... 21
Steps need to be taken ..... 21
Conclusion ..... 22

## Organization

BRAC University (BRACU) was established in 2001. It follows a liberal arts approach to education which nurtures fresh ideas and gives new impetus to the field of tertiary education. It ensures a high quality of education and aims to meet the demands of contemporary times. Building on BRAC's experience of seeking solutions to challenges posed by extreme poverty, BRACU hopes to instill in its students a commitment to working towards national development and progress. BRACU is accredited by the University Grants Commission (UGC) and approved by the Ministry of Education, Government of Bangladesh.

### Mission

The mission of BRAC University is to foster the national development process through the creation of a center of excellence in higher education that is responsive to society's needs, and able to develop creative leaders. It actively contributes to learning and the creation of knowledge.

### Goal

The goal of the University is to provide an excellent broad-based education with a focus on professional development for students, in order to equip them with the knowledge and skills necessary for leading the country in its quest for development. Along with this, the University provides an environment for faculty development to ensure a dynamic teaching environment. Faculty will be provided with an environment in which they can further their teaching-learning abilities and contribute to the creation of new knowledge by developing and using their research skills.

### Organizational Structure

The Honorable President of the People's Republic of Bangladesh is the Chancellor of BRAC University. The Board of Trustees is the highest policy making body of BRAC University and is responsible for ensuring the highest level of educational and administrative standard at BRAC University. A number of committees assist the Board in matters essential to the smooth functioning of the University. The committees are: Syndicate, Academic Council, Course Committee, Finance Committee, Selection Committee, Audit Committee, Student Affairs Committee, Disciplinary Committee, Committee on University Development and Committee on Medical Facilities.

## Programs

BRACU has thirty two academic programs, among these sixteen are undergraduate programs and rests are postgraduate programs. BRACU has trimester system except pharmacy.

The undergraduate programs are

- BACHELOR OF SOCIAL SCIENCES IN ANTHROPOLOGY
- BACHELOR OF SCIENCE IN APPLIED PHYSICS & ELECTRONICS
- BACHELOR OF ARCHITECTURE
- BACHELOR OF SCIENCE IN BIOTECHNOLOGY
- BACHELOR OF BUSINESS ADMINISTRATION (BBA)
- BACHELOR OF SOCIAL SCIENCE IN ECONOMICS
- BACHELOR OF ARTS IN ENGLISH
- BACHELOR OF SCIENCE IN COMPUTER SCIENCE & ENGINEERING
- BACHELOR OF SCIENCE IN COMPUTER SCIENCE
- BACHELOR OF SCIENCE IN ELECTRONIC AND COMMUNICATION ENGINEERING
- BACHELOR OF SCIENCE IN ELECTRICAL AND ELECTRONIC ENGINEERING
- BACHELOR OF LAWS [LL. B. (Hons.)]
- BACHELOR OF SCIENCE IN MATHEMATICS
- BACHELOR OF SCIENCE IN MICROBIOLOGY
- BACHELOR OF PHARMACY (HONS)
- BACHELOR OF SCIENCE IN PHYSICS

The postgraduate programs are:

- EXECUTIVE MBA
- M.S. IN BIOTECHNOLOGY
- M.SC./M.ENGG. IN COMPUTER SCIENCE AND ENGINEERING
- MA IN ENGLISH
- MA IN GOVERNANCE AND DEVELOPMENT
- MASTERS IN PROCUREMENT AND SUPPLY MANAGEMENT
- MA IN TESOL (TEACHING ENGLISH TO SPEAKERS OF OTHER LANGUAGES)
- MASTER IN COMPUTER APPLICATIONS
- MASTER IN DISASTER MANAGEMENT
- MASTER OF BUSINESS ADMINISTRATION

- MASTER OF BANK MANAGEMENT
- MASTER OF DEVELOPMENT STUDIES
- MASTER OF PUBLIC HEALTH
- MASTER OF SCIENCE (M. SC.)/MASTER OF ENGINEERING (M. ENGG.) IN ELECTRICAL AND ELECTRONIC ENGINEERING
- MASTERS (MED)/POSTGRADUATE DIPLOMA IN EDUCATIONAL LEADERSHIP & SCHOOL IMPROVEMENT
- MASTERS IN DEVELOPMENT MANAGEMENT AND PRACTICE
- MASTERS IN EARLY CHILDHOOD DEVELOPMENT

There are some other diplomas and certificates courses offered by BRAC University. They are

- DIPLOMA, ADVANCED DIPLOMA & PROFESSIONAL DIPLOMA OF THE CHARTERED INSTITUTE OF PROCUREMENT & SUPPLYING (CIPS)
- CERTIFICATE PROGRAMME ON ENVIRONMENTAL MANAGEMENT GOVERNANCE (EMG)
- CERTIFICATE IN CONSTRUCTION MANAGEMENT
- POST GRADUATE DIPLOMA IN BANK MANAGEMENT AND IT
- POST GRADUATE CERTIFICATE ON MANAGEMENT OF LAND ACQUISITION, RESETTLEMENT AND REHABILITATION (MLARR)
- POST GRADUATE DIPLOMA IN DISASTER MANAGEMENT
- POST GRADUATE DIPLOMA IN EDUCATIONAL LEADERSHIP & SCHOOL IMPROVEMENT

## Institutes and Schools

**BRAC BUSINESS SCHOOL**

The BRAC Business School (BBS) offers an undergraduate program (BBA, Bachelor of Business Administration) and three graduate programs (MBA, Masters of Business Administration; EMBA, Executive Masters in Business Administration; and MBM, Masters of Bank Management). The areas of specialization of the school are:

- Accounting
- Finance
- Banking and Insurance
- Human Resource Management
- Marketing
- Computer Information Management

- E-Business
- Entrepreneurship, and
- Operations Management

The school offers an undergraduate program (BBA, Bachelor of Business Administration) and two graduate programs (MBA, Masters of Business Administration and EMBA, Executive Masters in Business Administration). The areas of specialization of the school are Accounting, Finance, Banking and Insurance, Human Resource Management, Marketing, Computer Information Management, E-Business, Entrepreneurship, and Operations Management.

**BRAC INSTITUTE OF GOVERNANCE AND DEVELOPMENT**

BRAC Institute of Governance and Development (BIGD) is a resource center that promotes research and develops knowledge on practical solutions to issues of poverty, inequity and social injustice. At the core of BIGD's work are several academic courses, which include both classroom teaching and fieldwork experience:

Masters in Development Studies (MDS)

MA in Governance and Development (MAGD)

Masters in Procurement and Supply Management (MPSM)

Masters in Development Management and Practice (MDMP)

Postgraduate Certificate Course on Management of Land Acquisition, Resettlement and Rehabilitation (MLARR)

Microfinance: An Introductory Course

Applied Social and Marketing Communication: A Short Course

**JAMES P GRANT SCHOOL OF PUBLIC HEALTH**

The James P Grant School of Public Health (JPGSPH) at BRAC University was established in 2004 as an international educational and research institution focusing on the integral areas of teaching, research, and services. The goal of the School is not only to impart knowledge but also to act as a centre of excellence in knowledge creation through research and training that connect with practice.

The School's guiding vision - "knowledge and know-how for health equity" - draws on the inspirational leadership of James P. Grant, former executive director of UNICEF, after whom the School is named. The three primary areas of activity in the School are related to education, research and advocacy.

Aside from the flagship educational programmes, i.e. Master of Public Health (MPH), JPGSPH also provides public health short courses for health professionals through the Continuing Education Programme (CEP). Additionally, JPGSPH possesses a burgeoning research portfolio conducting innovative and pioneering studies on public health issues funded by multiple international donors. JPGSPH also offers services in the form of training, advocacy workshops, and seminars with a special focus on the rights of the marginalized and vulnerable population of Bangladesh.

**BRAC INSTITUTE OF LANGUAGES**

BRAC Institute of Languages (BIL) offers well-designed, comprehensive courses ranging from the pre-intermediate to the upper-intermediate level in order to facilitate the English language requirements of the university students. Besides English, BIL currently offers the modern languages Bangla, German, Chinese, French, Korean and Spanish to both its students and other professionals.

As a language institute, BIL has also decided to contribute to the improvement of language teaching in Bangladesh, and thus introduced the post-graduate degree course, Masters (MA) in TESOL, for currently practicing teachers and language practitioners. Interested teachers can also avail of other programs such as "Certificate in TESOL" and "Diploma in TESOL" which are also pre-requisites for the MA in TESOL course.

**BRAC INSTITUTE OF EDUCATIONAL DEVELOPMENT**

Since its inception it has been contributing to the overall improvement of the national education system in Bangladesh. BRAC Institute of Educational Development (BIED) runs two academic programmes, the Masters of Education (MEd)/ Post-Graduate Diploma (PGD) in Educational Leadership, Planning, and Management as well as the Masters in Science

(MSc)/PGD in Early Childhood Development. BIED also runs short courses for government officials who share our vision of bringing positive change to classroom teaching, learning, and management.

**SCHOOL OF ENGINEERING AND COMPUTER SCIENCE**

The School of Engineering and Computer Science embodies BRAC University's tradition of excellence as a leader in engineering education and research. The undergraduate and graduate programs offered by this School prepare students to be well-qualified for academia and industry, and to apply engineering principles across a wide range of disciplines.

The Department of Electrical and Electronic Engineering (EEE) and the Department of Computer Science and Engineering (CSE) operate together under this school. The EEE Department offers two undergraduate programs: Bachelor of Science in Electrical and Electronic Engineering (BSEEE) and Bachelor of Science in Electronics and Communication Engineering (BSECE), and the CSE Department offers Bachelor of Science in Computer Science (BSCS) and Bachelor of Science in Computer Science and Engineering (BSCSE). The School of Engineering and Computer Science has also expanded its curriculum to graduate levels by offering three graduate programs: Master of Science (M.Sc.) in Electrical and Electronic Engineering, Master of Engineering (M.Engg.) in Electrical and Electronic Engineering and Master of Computer Applications (MCA). Furthermore, the school is running a training program for CISCO Certified Network Associate (CCNA) under the CISCO Networking Academy in BRAC University. Besides academic programs, the School of Engineering and Computer Science especially encourages undergraduate and graduate students to engage in research activities. Under the patronization of the School, the Network Research Group is exploring different characteristics of wireless and wired networks such as security, channel optimization, and performance enhancement. The Control Application Research Group (CARG) has initiated research with Dhaka Power Distribution Company Ltd (DPDC) on the Supervisory Control and Data Acquisition (SCADA) system to analyze and improve their system, and is also working on implementing several solar power projects

**SCHOOL OF LAW**

The School of Law at BRAC University is a gateway through which students are prepared for careers in law, in administrative services, the judiciary and in the development sector. The four-year undergraduate programme at the School of Law culminates into a Bachelor of Laws (LL.B.) degree for successful students. Although the primary emphasis of the programme is on law and the legal profession, given that law is intertwined with economics, development, business and sociology, it also prepares students who are inclined to seek professions in other disciplines.

## Departments

**ARCHITECTURE**

The department offers following programs:

- Bachelor of Architecture
- Certificate in Construction Management
- Master in Disaster Management

The department undertakes research programs in different areas. It has done so in association with the Research and Education division of BRAC, the British Council, the University of Manchester, Loughborough University, Hoge School Van Amsterdam etc.

**COMPUTER SCIENCE AND ENGINEERING**

The undergraduate and graduate programs offered by this school prepare students to be well-qualified for academia and the industry, and to apply engineering principles across a wide range of disciplines. The CSE Department offers:

- Bachelor of Science in Computer Science (BSCS) and
- Bachelor of Science in Computer Science and Engineering (BSCSE)

The department has also expanded its curriculum to graduate levels by offering three graduate programs:

- Master of Science (M.Sc.) in Computer Science and Engineering
- Master of Engineering (M.Engg.) in Computer Science and Engineering, and
- Master of Computer Applications

**ECONOMICS AND SOCIAL SCIENCES**

Since its establishment, the department has given special attention to critical pedagogical methods in and outside classroom. An increasing number of students from other departments are opting to double major in Economics or to minor in Economics and Sociology.

The department offers an undergraduate degree in Economics, minors in Economics and Sociology, and a postgraduate degree in Applied Economics. From 2013, the department is also offering an undergraduate degree and a minor in Anthropology.

**ELECTRICAL AND ELECTRONIC ENGINEERING**

The Electrical and Electronic Engineering (EEE) department offers two undergraduate degree programs:

- Bachelor of Science in Electrical and Electronic Engineering and
- Bachelor of Science in Electronic and Communication Engineering

It also offers two graduate degree programs:

- Master of Science in Electrical and Electronic Engineering and
- Master of Engineering in Electrical and Electronic Engineering

Besides the academic programs, the department actively encourages both undergraduate and graduate students to engage themselves in research. There are several research groups operating under the EEE department at the moment as mentioned below.

**ENGLISH AND HUMANITIES**

The Department fosters the imaginative, observational, analytical and communicative skills of its students through its three major streams: Literature, Linguistics & ELT and Media. The Department also offers a Minor programme in History, which helps the students to contextualize their learning.

The postgraduate programme for the degree of M.A. in English has two streams: Literature and Linguistics & ELT.

### MATHEMATICS AND NATURAL SCIENCES

MNS Department has been providing quality education in basic and applied sciences to the students of different disciplines of BRACU including its own. Apart from offering courses in physical and life sciences like physics, chemistry, biology, biotechnology, microbiology and also courses in mathematics, statistics, economic geography, environmental sciences, MNS Department also has its own undergraduate degree programs in physics, applied physics and electronics, microbiology, biotechnology and mathematics. It also offers a Master's program namely, MS in Biotechnology.

### PHARMACY

Bachelor of Pharmacy (Honours) curriculum in BRAC University is to introduce beginning pharmacy students to the technologic and scientific principles underlying the preparation of dosage forms and drug delivery systems and to their use in patient care. Through an integrated course curriculum students will gain an understanding of the interrelationships between physical pharmacy principles, biopharmaceutics and pharmacokinetics, dosage form design, product formulation, small- and large-scale product manufacture, and the clinical application of pharmaceuticals in patient care.

## Centre and Initiatives

### CENTRE FOR CLIMATE CHANGE AND ENVIRONMENTAL RESEARCH (C3ER)

Since its inception, BRAC University has conducted a series of cross-sectoral research on climate change and disaster management in direct collaboration with BRAC. To coordinate and manage these different activities, the Syndicate and the Board of Trustees of BRAC University have accorded for establishment of a research center titled "Centre for Climate Change and Environmental Research (C3ER)". The Centre establishes a synergy between BRACU and BRAC in the field of climate change and other environmental issues.

### CENTRE FOR ENTREPRENEURSHIP DEVELOPMENT

Centre for Entrepreneurship Development (CED) started its journey in April 2011 with the view to encourage Bangladeshi entrepreneurs and engender entrepreneurial knowledge and skill so that they can develop and grow their own businesses.

## CONTROL AND APPLICATIONS RESEARCH CENTRE

The Control & Applications Research Centre (CARC) has expertise and activities in an area of systems and control engineering. CARC has a strong practical focus to the work, and many of the projects involve close collaboration with industrial organizations. We emphasis upon the application requirements and exercise established theoretical techniques to provide solutions through technological demonstration.

## PROFESSIONAL DEVELOPMENT CENTRE

The Professional Development Centre (PDC) is an innovation of BRAC University dedicated to promoting excellence in education through shared understanding and best practice. The centre was previously known as the Teaching & Learning Centre, opened in 2006. The PDC strives to build a creative environment of pedagogical development and research that fosters innovation across the University in collaboration with faculty and administrative staff. The focus of the centre is to keep the campus community updated with pedagogical developments, coordinate academic resources, support professional development and contribute to successful student learning. From group events to personalized attention, the PDC supports measurable effectiveness in faculty development, course instruction and assessment, scholarly research, and innovation in education technologies. Our expanding activities and services include orientations, workshops and seminars, individual consultations, pedagogical research, teaching courses and programme design.

## CERTIFICATE PROGRAMME ON ENVIRONMENTAL MANAGEMENT GOVERNANCE (EMG)

The BRAC Institute of Governance and Development (BIGD), BRAC University is offers Certificate Programme on Environmental Management and Governance jointly with the Centre for Natural Resource Studies of the University of Manitoba, Canada. The main purpose of the certificate programme is to sensitise and enhance the capacity of participants on key environmental governance issues related to natural resources and environment management. The certificate course is an intense programme which would provide opportunities to the participants to be trained with key concepts of environmental issues and concerns, management system, environmental governance, implementation methods and procedures.

# Information Security

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical). The term information security has different interpretations based on what era the term describes. It is more appropriate to call it computer and network security. Computer and network security are built in three pillars, commonly referred to by the CIA acronym

- Confidentiality
- Integrity
- Availability

Information is confidential if it stays obscure to all but those authorized to use it. Information has integrity as long as it remains identical to its state when the last authorized user finished with it. Information is available when it is accessible by authorized user in a convenient format and within reasonable time.

## Threats to security

We can categorize the threats by discussing vulnerabilities and threats. We also will describe viruses and other malwares later.

### Vulnerabilities

Vulnerabilities can be defined as the point where a system is susceptive to attack. There are few major vulnerabilities of a system.

**Physical vulnerabilities**

Your buildings and equipment rooms are vulnerable. Intruders can break into your server room, just as they can break into your home. Once in, they can sabotage and vandalize your network equipment, and they can steal backup media and printouts, or obtain information that will allow them to more easily hack their way in at a later time.

Locks, guards, and biometric devices (devices that test a physical or behavioral trait for example, a fingerprint, a voiceprint, or a signature and compare it with the traits on file to determine whether you are who you claim to be) provide an important first defense against break-ins. Burglar alarms and other ordinary types of protection are also effective deterrents.

**Natural vulnerabilities**

Computers are very vulnerable to natural disasters and to environmental threats. Disasters such as fire, flood, earthquakes, lightning, and power loss can wreck computer and destroy data. Dust, humidity, and uneven temperature conditions can also do damage.

In areas where obtaining stable power is a problem, facilities employ back-up generators. These can also help during times of extreme weather. Localized protection can be obtained through installing an uninterruptible power supply (UPS). A properly sized UPS will keep a computer energized long enough to shut down properly and without data loss, and provide power conditioning as well. Dust and other hazards are usually controlled by proper filters on the air conditioning and heating systems. If the environment itself tends to be dusty, a simple cloth cover can protect the computer when not in use. Do not cover a computer while it is operating, however, to avoid blocking the internal cooling fans and let the case radiate excess heat. Even temperature will help eliminate some problems, as well. The components and cards in a computer may expand and contract at different rates; they can become loose in their sockets. Avoid dampness in areas where removable media, such as CDs, DVDs, and backup tapes, are stored; mold and fungus are lethal to some media.

**Hardware and software vulnerabilities**

Certain kinds of hardware failures can compromise the security of an entire computer system. If protection features fail, they wreak havoc with system, and they open security holes. It is also possible to open some "locked" systems by introducing extra hardware, or to use external devices to make a copy of the contents of disks or memory.

Software failures of any kind may cause system to fail, open system to penetration, or simply make the system so unreliable that it can't be trusted to work properly and efficiently. Thriving exploration into vulnerabilities by the hacking community means that exploits will be published in online forums, paving the way for those who wish to write and publish viruses or other malicious software to do so. In particular, bugs in security features can open the floodgates to intrusion.

Even if individual hardware and software components are secure, an entire system can be compromised if the hardware components are connected improperly or if the software isn't installed correctly.

**Emanation vulnerabilities**

All electronic equipment emits electrical and electromagnetic radiation. Electronic eavesdroppers can intercept the signals emanating from computers, networks, and wireless

systems, and decipher them. The information stored and transmitted by the systems and networks then becomes vulnerable.

**Communications vulnerabilities**

If computer is attached to a network or if it can be accessed by a dial-in modem or over the Internet, you greatly increase the risk that someone will penetrate your system. Messages can be intercepted, misrouted, and forged. Communications lines connecting computers to each other, or connecting terminals to a central computer, can be tapped or physically damaged.

**Human vulnerabilities**

The people who administer and use computer system represent the greatest vulnerability of all. If your administrator is poorly trained, or decides to take to a life of crime, your network is in grave peril. Ordinary computer users, operators, and other people on staff can also be bribed or coerced into giving away passwords, opening doors, or otherwise jeopardizing security in your system.

**Exploiting vulnerabilities**

There's a lot of variation in how easy it is to exploit different types of vulnerabilities. For example, tapping a wireless network can require nothing more than special software installed on a laptop. Logging into a system that has no password protection, minimal controls, or inadequate password policies (e.g., allowing users to leave passwords on sticky notes at their workstations) is almost as easy. Tapping an encrypted fiber-optic communications link, on the other hand, or intercepting emanations from TEMPEST-shielded equipment is much more difficult, even for a dedicated intelligence operation

## Threats

Threats can be defined as possible danger to a system. Threats fall into three main categories: natural, unintentional, and intentional.

**Natural and physical threats**

These threats imperil every physical plant and piece of equipment: fires, floods, power failures, and other disasters. We can't always prevent such disasters, but we can find out quickly when one occurs (with fire alarms, temperature gauges, and surge protectors). We can minimize the chance that the damage will be severe (e.g., with certain types of sprinkler systems).

**Intentional threats**

These villains come in two varieties: outsiders and insiders. Some types of attacks are feasible only for certain types of attackers.

Outsiders may penetrate systems in a variety of ways: simple break-ins of buildings and computer rooms; disguised entry as maintenance personnel; anonymous, electronic entry through modems and network connections; and bribery or coercion of inside personnel. Although most security mechanisms protect best against outside intruders, survey after survey indicates that most attacks are by insiders. Estimates are that as many as 80 percent of system penetrations are by fully authorized users who abuse their access privileges to perform unauthorized functions. As Robert H. Courtney Jr. put it, "The enemy is already in we hired them." There are a number of different types of insiders. The fired or disgruntled employee might be trying to steal; more likely, he's just trying to wreak revenge by disrupting office operations. The coerced employee might have been blackmailed or bribed by foreign or corporate enemy agents. The greedy employee might use her inside knowledge to divert corporate or customer funds for personal benefit. The insider might be an operator, a systems programmer, or even a casual user who is willing to share a password.

**Unintentional threats**

Ignorance creates dangers: for example, a user or a system administrator who hasn't been trained properly, who hasn't read the documentation, and who doesn't understand the importance of following proper security procedures. A user might inadvertently delete a file, or a system administrator might change the protection on the password file or on critical system software, locking out programs and applications that need to access that data.

## Malicious Programs

In this section I will try to describe some malicious programs,

**Virus**

A virus is a code fragment that copies itself into a larger program, modifying that program. Unlike a worm, described in the next section, a virus is not an independent program but depends upon a host program, which it infects. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces. After seeing to its own reproduction, it then does whatever dirty work it carries in its programming, or payload.

**Worms**

A worm is an independent program that reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Like a virus, a worm compounds the damage it does by spreading rapidly from one site to another. Unlike a virus, which attaches itself to a host program, a worm keeps its independence; it usually doesn't modify other programs. Like a virus, however, a worm can include malicious instructions that cause damage or annoyance, in

addition to whatever inconvenience it causes by tying up the resources of the network as it maintains and reproduces itself.

**Trojan Horses**

A Trojan horse is a code fragment that hides inside a program and performs a disguised function. In classical mythology, a Trojan horse was a large hollow horse made of wood by Odysseus during the Trojan War. The Greeks hid soldiers inside the horse and left it at the gates of Troy. After the Trojans were persuaded to bring the horse inside the gates, the hidden soldiers opened the doors for the rest of the army, which attacked the city and won the war.

In the modern computer world, a Trojan horse hides in an independent program that performs a useful or appealing function or appears to perform that function. Along with the apparent function, however, the program performs some other unauthorized operation. A typical Trojan horse tricks a user into running a program, often an attractive or helpful one. When the unsuspecting user runs the program, it does indeed perform the expected function. But its real purpose is often to penetrate the defenses of the system by usurping the user's legitimate privileges and thus obtaining information that the penetrator isn't authorized to access. An example of this would be the modern rootkit, which is a script that controls a small suite of programs that create an administrative level account on the targeted system, and then create a backdoor, an unmonitored entrance way that evades the security mechanisms, through which the attacker can later gain convenient access. Trojan horses are often hidden in programs that entice users by displaying information about new system features or by hiding in downloadable applications or games.

Many web site operators today insert Trojan horses that create content that pops up on your screen while you are doing other functions. While the marketers may claim they are merely displaying additional advertisements that may be in sync with what you were currently browsing, what they are actually doing is monitoring your actions, and then sending out codes over your network that pull in content you did not request, and then put it in front of you. For this service they charge the content owner a fee.

**Bombs**

A bomb is a type of Trojan horse, used to release a virus, a worm, or some other system attack. It's either an independent program or a piece of code that's been planted by a system developer or a programmer. A bomb works by triggering some kind of unauthorized action when a particular date, time, or condition occurs.

**Trap Doors**

A trap door, or a back door, is a mechanism that's built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system, circumventing normal system protection. Unlike a logic bomb, which usually explodes in someone else's system, a trap door gives the original designer a secret route into the software.

Sometimes, programmers leave trap doors (entry points) in a program to allow them to test the program, or monitor its operation, without having to follow what may be cumbersome access rules or security measures. These trap doors also provide a way to get into the program in case there's a problem with the access routines. Although such trap doors are ordinarily removed before the program is shipped to the customer, sometimes they're left in the code by accident or by design.

**Spoofs and Masquerades**

A masquerade is a generic name for a program that tricks an unsuspecting user into giving away privileges. Often, the ruse is perpetrated by a Trojan horse mechanism in which an authorized user is tricked into inadvertently running an unauthorized program. (The Trojan horse login described earlier is an example of such an attack.) The program then takes on the privileges of the user and may run amuck!

A spoof, on the other hand, is an important technique used for misdirection and concealment. Sometimes, a communication that the sender wishes to transmit anonymously is tagged with a false return address. Spoofing return addresses in this way is one of the techniques used to create unsolicited junk email advertisements (spam) with no way to track down the offending sender.

**Other Modern form of Attack**

Denial of service attack (DoS): Attack that produces so many requests of system resources in the computer under attack such as calls to the operating system, or opening dialogs with other machines and then hanging onto the line to tie it up that normal functions on the targeted computer are overwhelmed and cease.

Distributed DoS attack (DDoS): DoS attack launched from many different computers, usually zombies hijacked for this purpose.

Exploit: Malware that capitalizes on known or undiscovered vulnerabilities, which are bugs or weakness in software applications or operating systems.

Rootkit: Malware, usually a small suite of programs, that install a new account or steal an existing one, and then elevate the security level of that account to the highest degree (root for Unix, Administrator for Windows) so that attackers can do their will without obstruction.

Script: File containing specific instructions of the attacker and commands to make them occur.

Sniffer: An attack, usually a Trojan horse that monitors computer transactions or keystrokes. A keystroke logger, for instance, detects sensitive information by monitoring the user's keystrokes.

Zombie: A corrupted computer that is waiting for instructions and commands from its master, the attacker.

## Countermeasure

There are many programs that can help us keep viruses and other malware away from our system and can wipe out the critters if they gain access. Known as virus protection programs, these programs are available from both commercial and public domain sources. These products, and the system administration procedures that go along with them, have two overlapping goals: they don't let you run a program that's infected, and they keep infected programs from damaging your system.

### Firewalls

A firewall protects computer by examining each information packet that travels over the network. Clues to a packet's purpose can be read from its destination address. Firewalls contain a list of allowed and disallowed destinations and functions. If a packet is heading for a forbidden address or comes from one, the firewall stops it. If a packet is heading for a valid address, but its port identifier (the clue to packet function) is unknown or disallowed, the firewall stops that packet as well. Advanced firewalls even keep track of outgoing packets, and open up only if a packet is expected and returning.

### Antivirus

Virus protection software uses two main techniques. The first uses signatures, which are snapshots of the code patterns of the virus. The antivirus program lurks in the background watching files come and go until it detects a pattern that aligns with one of its stored signatures, and then it sounds the alarm and maybe isolates or quarantines the code. Alternatively, the virus protection program can go looking for trouble. It can periodically scan the various disks and memories of the computer, detecting and reporting suspicious code segments, and placing them in quarantine.

One problem with signature-based virus protection programs is that they require a constant flow of new signatures in response to evolving attacks. Their publishers stay alert for new viruses, determine the signatures, and then make them available as updated virus definition tables to their users. To access the new tables, users typically download them from the World Wide Web.

Of course, as the number of viruses increases (and it shows no signs of abating), the tables get progressively larger, making frequent updates somewhat of a chore. This is particularly a problem in the case of memory-limited devices such as palm-top computers or intelligent cell phones.

## Cyber Attack Globally

In this section I will discuss about the current state of information security. Information security is one of the most critical issues in modern era where internet of things (IoT) is reality. IoT can be defined as a system where all the daily objects are connected to network and able to send and receive data. If we look into this issue we can see some attacks (cyber-attack) were detectable most of the attacks was not detected. According to pwc state of information security survey 2016 only 38% attacks were detectable. According to the FireEye asia is the worst in term of discovering cyber attack.


Fig 1: Days taken to discover cyber attack

The good news is 91% companies have adopted risk based cyber security framework.

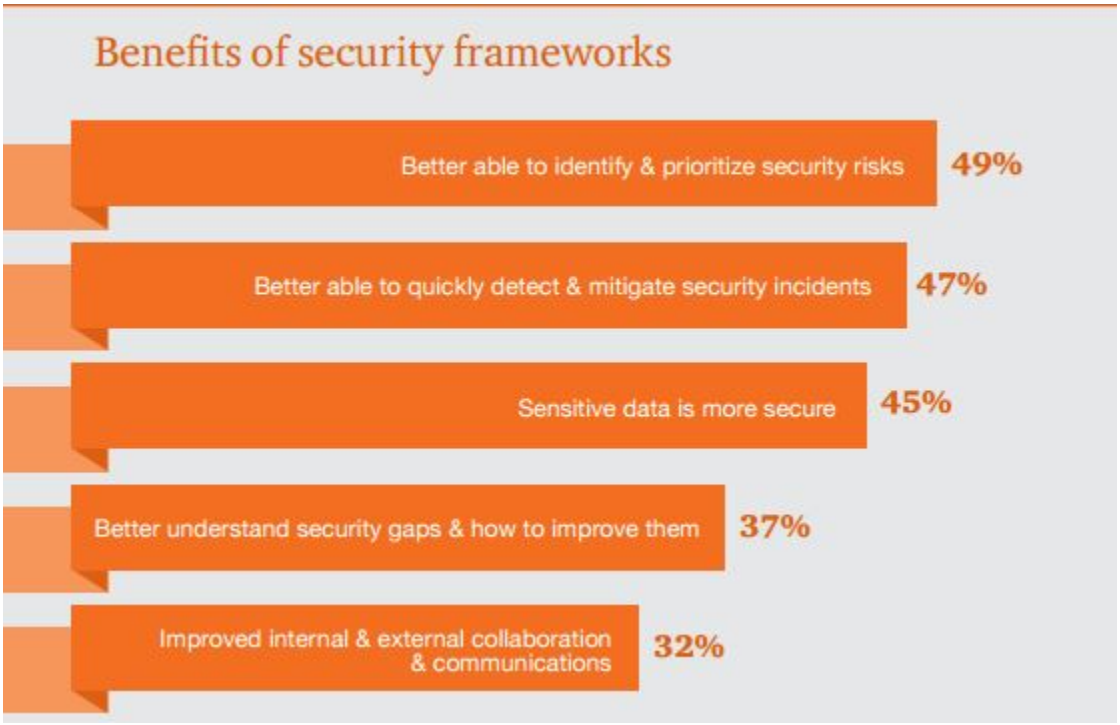


Fig. 2: Benefits of security framework

Another critical issue is authentication. Password is now more advanced. It can be one time password (OTP), biometric scan or magnetic card. 91% companies have adopted advanced authentication.


Fig 3: Benefits of advanced authentication

## Information Security in BRAC University

BRAC University uses many IT services to conduct its regular activities. HR and Accounts department have their own web based software which was developed by BRAC IT Services Limited. Academia is web based software for student management; it was maintained by BRAC IT Services Limited. There were various issues regarding this web based application. There were multiple incidents of data loss, but due to routine and multi-level back up policy. This software will be the main target if someone wants to change the grade sheet. Academia is a common platform and used widely in different institutions. It will be less difficult to attack this software. The major issue faced by the faculty is masquerade. In these type event faculty receives mail where he is told to click the content of the mail which leads to file loss and password breach. BRAC University uses zimbra mail server which is open source email service. Due to its nature as open source it is frequently used for phishing. It is highly vulnerable for security attack. The university uses different antivirus to different pc, it depends on the IT Officer which one to use. BRAC University has TSR folder which is domain based file transfer service to share file between student and faculty members.

If we examine physical state of network devices (i.e wifi router and switch) not all devices situated in ideal location. For example switch box in some location is situated inside kitchen where ideal temperature for switch operation may not be ensured.

The main users of PC are student (computer lab), faculties, classrooms and staff member. Some computers are old and running operating systems which are obsolete. More than 2000 students uses lab pc daily which are vulnerable to malware. Many PCs are infected with worms like sort cut, hidden file etc.

## Steps need to be taken

According to my observation few steps need to be taken to improve information security at BRAC University.

1. Student management software academia should improve or replaced
2. Use more filter in mail server
3. Zimbra mail server should be replaced
4. Buy antivirus and develop new policy regarding uses of antivirus
5. TSR should be integrated with student management or use Google Classroom (Free)
6. Network devices should be kept in ideal environment
7. Routine audit should occur frequently
8. Old devices and operating system should be replaced by new
9. IT Officers should be trained to provide systematic solution
10. Create a new IT policy framework

## Conclusion

Information security in any institution is essential in modern world. It affects everyone because how widely we use internet. It will be wrong if we consider this topic is insignificant in educational institution. In past, all hacker practiced there skill by attacking educational institutions. Due to lack of discovery many of those incidents are still unknown. IT and systems department of BRAC University should consider threats are likely and I believe it is right time to put more focus in information security.

# Reference


1. ISO/IEC 27001. Information technology - security techniques - information security management systems - requirements. On-line. 3.1.2
2. Mohammad Mannan Atieh Saberi Pirouz, Vladimir Rabotka. Friendlymail:Condential and veried emails among friends. Concordia University, Mon-treal, Canada, March 14, 2014. 3
3. JeF Bardin. A standard, a framework or a standard framework? On-line available, April 2009. Retrieved on 15/10/2014. 3.1.2
4. Matthew Campagna. Aws key management service cryptographic details. Technical report, Amazon Web Services, November 2014. 4.2
5. Steve Durbin. Cyber crime: battling a growth industry. Financial Times, September 5 2014. 3.1.1
6. Security for Industrial Automation, Control Systems: System Security Requirements, and Security Levels. Ansi/isa-62443-3-3 (99.03.03)-2013, 2013.3.1.2