VIT | Vidyalankar Institute of Technology

Accredited A+ by NAAC

University Paper Solution

- December 2019 exam

Name	Harshada Rajale
Designation	Assistant Professor
Department	Electronics and Telecommunication
Class	B.E. - C
Subject	Cyber Security and Laws

BE – VII – CBCGS – All Branches. – NOV 2019

(3 Hours) (Total Marks : 80)

26/11/2019

N.B: 1) Q.1 is compulsory.
2) Attempt any THREE questions from the remaining questions.
3) Assume suitable data if necessary.

Q.1 Attempt any four :

a) Compare active attacks vs Passive attacks. [5]

b) Explain various types of key-loggers in brief. [5]

c) Classify the cybercrimes and explain any one briefly. [5]

d) Explain how the appeals can be made under The IT ACT 2000. [5]

e) Write brief note on : Cyber-terrorism. [5]

Q.2 a) How criminals plan the attack? Discuss various steps involved [10]

b) Explain how Intellectual property laws protect the rights of the owner of the intellectual Property. 146 [10]

Q.3 a) Compare Vishing, Phishing and Smishing in cyber security. [10]

b) What is E-commerce? Explain different types of e-commerce with suitable examples. 132 [10]

Q.4 a) What is Bluetooth hacking? Explain Bluetooth hacking tools in brief. 73 [10]

b) How the Indian penal code IPC 1860 addresses cybercrime? [10]

Q.5 a) Discuss basic security precautions to be taken to safeguard Laptops and wireless devices. [10]

b) What is E-contract? Discuss E-contract Act 1872. [10]

Q.6 Write short note on (Any 2) [20]

1) Computer Sabotage.
2) Indian Information Technology Act 2000
3) Write key IT requirements for SOX and HIPAA.

VIT Vidyalankar Institute of Technology

End Semester Examination (MU)

Evaluation of University Question Paper Solution Prepared by Faculty

Subject (Write in full) : CYBER SECURITY AND LAWS (Regular / ~~KT~~)

Exam : ~~May 20~~ ____ / Nov. 20 19 Exam Date : 26/11/2019 Q. Paper Code : 77181

Department : EXTC Year : ~~FE/SE/TE/BE/ME/MMS~~ Semester : VII Scheme : ~~CBSGS~~/CBCS

Handwritten Solution Prepared by : HARSHADA A. RAJALE

Name of the Subject Cluster : INFORMATION SECURITY

Name of the Cluster Mentor / Assessor : PROF. DILIP MOTWANI

1st Assessment :

Question No.	Marks Obtained						Total
1	(a)	(b)	(c)	(d)	(e)	(f)	
2	(a)	(b)	(c)	(d)	(e)	(f)	
3	(a)	(b)	(c)	(d)	(e)	(f)	
4	(a)	(b)	(c)	(d)	(e)	(f)	
5	(a)	(b)	(c)	(d)	(e)	(f)	
6	(a)	(b)	(c)	(d)	(e)	(f)	
Total (Out of marks)							

Signature of Assessor / Cluster Mentor : _____

2nd Assessment :

Question No.	Marks Obtained						Total
1	(a)	(b)	(c)	(d)	(e)	(f)	
2	(a)	(b)	(c)	(d)	(e)	(f)	
3	(a)	(b)	(c)	(d)	(e)	(f)	
4	(a)	(b)	(c)	(d)	(e)	(f)	
5	(a)	(b)	(c)	(d)	(e)	(f)	
6	(a)	(b)	(c)	(d)	(e)	(f)	
Total (Out of marks)							

Signature of Assessor / Cluster Mentor : _____

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

START WRITING HERE

Q.1 Attempt any four:

(a) Compare active attacks vs Passive attacks

Basis for comparison	Active Attack	Passive Attack
① Basic	Active attack tries to change the system resources or affect their operation.	Passive attacks tries to read or make use of information from system but does not influence system resources.
② Modification in information	occurs	Does not take place.
③ Harm to the system	Always causes damage to the system.	Do not cause any harm.
④ Threat to	Integrity & availability	Confidentiality
⑤ Attack awareness	The entity gets informed about attack.	Entity is unaware about the attack.
⑥ Tools	BuiltWith, WHOIS, NS lookup, etc	Arping, Dig, Hping, etc

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

⑥ Task performed by the attacker	The transmission is captured by physically controlling the link portion.	Just need to observe the transmission
⑦ Emphasis is on	Detection	Prevention.

(b) Explain various types of key-loggers in brief.

A Key-logger is a malicious computer program which records every keystroke made by a computer user.

Employers use keyloggers to keep a watch over employees but cybercriminals use keyloggers to gain access to confidential information like passwords & other critical data.

(A) Software Keyloggers

They are software programs that track the activities (key pressed) of a keyboard.

They are usually located between the operating system & keyboard hardware.

Examples of software Keyloggers are listed below:

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

(a) SC- Keylog PRO :-

SC- Keylog PRO is a powerful digital surveillance monitor that logs computer activity for later review

(b) Stealth keylogger :-

It is a software keylogger that can run while being completely invisible to users.

(c) KyB Spy :-

Along with keyboard tracking, it is capable of recording language specific character.

(d) Spy Buddy

It is a powerful keylogger software which allows you to monitor all areas of your PC & track every action.

(e) Elite keylogger

It is one of the best keyloggers for remaining undetected.

(B) Hardware Keyloggers

Hardware based keyloggers can monitor your activities without any software being installed at all.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

(a) Keyboard hardware

These loggers take the form of piece of hardware inserted somewhere between computer keyboard & the computer, typically along the keyboard's cable connection.

(b) Wireless keyboard sniffers

It is possible for sgs sent from a wireless keyboard to its receiver to be intercepted by a wireless sniffer.

(c) Keyboard overlays.

Overlays are popular in ATM theft cases where thieves capture a user's PIN number. Each keypress on the keyboard of ATM gets registered by these keyloggers.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q	Classify the cybercrimes & explain any one briefly.

There are many types of cybercrimes that prevail in the system depending on the target & nature of the crime. The cybercrimes can be broadly classified into four major categories described as follows:

(A) Cyber crime against Individual

It involves actions that are taken to harm an individual

1. Online Frauds
2. Phishing
3. Spamming
4. Cyber defamation
5. Cyber Stalking
6. Computer Sabotage
7. Pornographic offenses
8. Password sniffing

(B) Cybercrime against Organization

Cybercrimes that target an organization are of various kinds discussed

1. Unauthorised access.
2. Password sniffing
3. DOS attacks
4. Virus attacks
5. Email Bombing
6. Salami Attack.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

⑦ Logic Bomb
⑧ Trojan Horse
⑨ Data Diddling

② Crimes Emanating from Usenet Newsgroup

Acts such as industrial spying, computer net intrusions or software piracy come under this category of crime

① Industrial spying
② Computer net intrusion
③ Software Piracy

① Cyber crime against Society

① Forgery
② Cyber terrorism
③ Web Jacking

③ Cyber crime Against Property.

Some of the popular crimes against property are credit card frauds, intellectual property crimes & Internet time theft

① Credit card Frauds.

A theft or fraud committed using or involving a credit card as a fraudulent source of funds in a transaction

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
		② Intellectual property crimes Cyber theft of Intellectual property (IP) means stealing of copyrights, trade secrets, patents etc, using the Internet & computers. Frequently stolen forms of IP are copyrights & trade secrets. For example, stealing of software or a unique recipe of a well-known dish is a kind of IP crime. ③ Internet Time Theft. Internet Time / Bandwidth theft is a crime where the Internet connection of a victim is used by a criminal who gain access to the victims account like username & password by fraudulent means. The criminal can thus, use the victim's Internet account for free Internet access, the cost of which will have to be borne by the victim
	④	Explain how the appeals can be made under the IT ACT 2000. ① Cyber crimes can be reported at the cyber cell established by the Police department in different cities.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

② The Information Technology Act, 2000 clearly states that when a cyber crime has been committed, it has a global jurisdiction, & hence, a complaint can be filed at any cyber cell.

② Complaints can be made anytime to the cyber police or crime investigation department either offline, online or by a calling at cyber crime helpline number.

③ As per section 78: Power to investigate offences, a police officer not below the rank of Inspector, can investigate any offence under IT Act 2000.

① Section 48: Establishment of Cyber Appellate Tribunal

This was established under ITA 2000, under section 48 by Central Government. Initially the Tribunal consisted of only one person who was referred to as Presiding officer appointed by CG. In section 49, it consists of Chairperson & a number of other members.

② Section 57: Appeal to Cyber Regulation Appellate Tribunal

It provides the right to appeal to

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Cyber Appellate Tribunal if any person is aggrieved by an order made by Controller or an adjudicating officer.
The Appeal may be filed within 45 days from date of communication of decision or order of Controller or adjudicating officer.

③ Section 58 :- Procedure & powers of the Cyber Appellate Tribunal

① As per the section 58 of IT ACT 2000, the Tribunal is not bound by the procedure laid down by the Code of Civil Procedure 1908.
② Instead, it is guided by the principles of natural justice which revolves around the premise that the authority should hear the person concerned before passing any decision, direction or order against him/her.
③ Section 58 also gives, the Cyber Appellant Tribunal powers that are vested in a civil court, as per the Code of Civil Procedure, 1908 & the proceedings before it is like a judicial proceeding.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

④ Section 62 : Appeal to High Court.

As per section 62, the IT ACT 2000 provides for any person aggrieved by any decision or order of the Cyber Appellate Tribunal, to appeal in High Court.

The appeal is to be filed within 60 days from the date of communication of the decision.

⑤ Write brief note on : Cyber terrorism.

① This term was coined in 1997 by Barry Collin, a senior research fellow at Institute for security & Intelligence, California.

② Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs & data which result in violence against non-combatant targets by sub national groups or clandestine agents.

③ Cyber terrorism is the use of the Internet to conduct violent acts that result in or cause threaten, loss of life.

④ It is also sometimes considered an act of Internet terrorism where

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
		terrorist activities include acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by means of tools such as computer viruses, computer worms, phishing, & other malicious software & hardware methods & programming scripts.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q.2 (a)	How criminals plan the attack? Discuss various steps involved.

① Criminals make use of many tools & techniques to locate the vulnerability of their target / victim.
② Attackers plan attacks in either passive or active mode.
③ They try to gain information about target in passive attacks. Whereas, through active attacks, they try to alter computer systems.
④ The following are three major ways/phases involved in planning of a cyber crime

Ⓐ Reconnaissance
Ⓑ Scanning & scrutinizing
Ⓒ Launching an Attack.

Ⓐ Reconnaissance

① In this phase, an attacker tries to explore & gain every possible information about system resources, vulnerabilities or services on victim's / target's system. This is referred as Foot printing
② The goals of attacker in this phase is to understand the system, personal information about the target, networking ports & services running on

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

those ports & any other related info.
In reconnaissance, information is gathered in active & passive phases.

- **Passive Attacks**

① They are used to gain information about individuals or organisations.
② They exploit confidential information.
③ Some of simple ways are given as follows:
- Use google or other search engines
- Social media
- Organisation website
- Blog or press release
- Job posting
- Network sniffing

④ Some of the famous tools of launching Passive attacks are
- CheckUserNames
- BuiltWith
- WHOIS
- Nslookup
- Traceroute
- emailtrackerPro
- HTTrack.

- **Active Attack**

① They are mostly manipulating or altering a system

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

② They have an effect on the integrity, authenticity & availability of data.

③ In this phase the attacker verifies & gathers the information (IP address, operating system, nlw range, hidden servers, personal information)

④ Following are some common tools used for launching active attacks.

- Arphound
- Arping
- Bing
- Dig
- Dsniff
- Mailsnarf
- Hmap
- Hping
- Urlsnarf
- NBT scan
- TCP dump
- TCP relay.

⑤ Scanning & Enumerizing

In this phase, the attacker collects the validity of information as well as finds out the existing vulnerability. This phase is also referred as "enumeration". The objectives of this phase are to:

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

① Validate user account & group
② Explore lists of nlw resources & shared nlw devices
③ Find different types of operating systems & applications running on a target system
It is a key phase before the actual attack takes place.

Various scanning techniques used by the attackers are stated as follows:

ⓐ Port scanning
Identify all ports, port status (open/closed), services running on those ports, etc.

ⓑ Network scanning
Understand & verify the IP address of the target & related nlw information before launching an attack

ⓒ Vulnerability scanning
Check & understand loopholes in the target system

ⓒ Launching an Attack
① Once step 2 is completed, the cyber attacker is ready to launch the attack to gain system information. The steps that will be followed

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
		Are as follows:-
		① Crack the password
		② Exploit the privilege
		③ Execute malicious commands
		④ Hide files
		⑤ Final but most important step- cover the track.
	Q.2(b)	Explain how Intellectual property laws protect the rights of the owners of the intellectual Property.
		① Intellectual property refers to the intangible property that is creation of the human mind.
		② The intellectual property rights aim to provide the innovators & creators legal protection for their ideas & creations.
		③ This may be done by copyrighting written works, applying for patents for inventions & trademarking brands, names & logos.
		④ Intellectual property encompasesses two types of right: Industrial property rights (trademarks, patents, geographical indicators, designations of origin, industrial designs & models, etc.) & copyright (literary,

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

dramatic, artistics & musical works, films.).

⑤ Types of Intellectual Property.

(i) Patents
(ii) Trade secrets
(iii) Trademarks
(iv) Geographical Indication.
(v) Industrial Designs
(vi) Copyright.

⑥ The Indian Information Technology Act, 2000 has no provision for the protection of intellectual property rights.

⑦ The Indian Copyright Act, 1957, deals with the protection of computer software & is inadequate to address all the aspects of Information Technology.

⑧ Indian Copyright Act, 1957

The Copyright Act 1957 (as amended by Copyright Act 2012) governs the subject of copyright law in India.

The Act defines the term "computer" & "computer program" in section 2.

Section 63B: Knowing use of infringing copy of computer programme to be an offence.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

(B) Patent Act, 1970

① The Patent Act 1970, came into force in the year 1972, amending & incorporating the existing laws relating to Patents & Designs act 1911 in India.

The Patent (Amendment) Act 2002 came into effect on 20th May 2003.

② Computer software is considered as an valuable property & forms a part of intellectual property.

However, the by itself is not patentable in India as there is no legal or conclusive definition of a software patent.

However the she can be patented if it is part of an invention that is both inventive & capable of industrial use.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q3(a)	Compare Vishing, Phishing & Smishing in cyber security.

(A) Vishing

Vishing is a criminal practice of using the telephone system to gain access to the personal & financial information of customers for purpose of committing fraud.

A typical process involves the following steps

① A war dialler is used to call numbers in a given region or a legitimate voice messaging system is compromised & calls are made with a list of phone numbers stolen from a financial institution.

② When a customer answers the call, an automated alerts the customer regarding fraudulent activity detected on his/her bank card or account.

③ The message instructs the customers to place a call to the bank immediately & provides a false phone number.

④ When victim calls the number the automated instructions request that he/she enters a credit card/bank account no. in keypad.

However, the call can also be used to harvest additional details such as

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

personal identification numbers, expiration dates, CVV number & DOB
⑤ As the customer enters the requested data the fraudster gets the information necessary to make fraudulent use of the card to access the account.
Steps to avoid vishing scams
(i) Never answer call from unknown number
(ii) Never share personal information over phone
(iii) Do not completely trust caller ID.
(iv) Avoid automated call
(v) Report the incident.

⑥ Phishing.
① Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords & credit card details by disguising oneself as a trustworthy entity in a electronic communication.
② Phishing Techniques
(a) URL manipulation
(b) Filter evasion
(c) Website forgery
(d) Search engine phishing
(e) Web based delivery

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

③ Phishing Scam Types :-
- (a) Session hijacking
- (b) Cross-site scripting
- (c) Malware-based phishing
- (d) Keyloggers based phishing
- (e) Spear phishing
- (f) Whale phishing
- (g) Vishing
- (h) Smishing.

④ Phishing Countermeasures:
- (i) Filter e-mail for phishing threats
- (ii) Update client-side operating systems, software & plug-ins
- (iii) Harden your clients
- (iv) Block Internet bound SMB & Kerberos traffic
- (v) Detect malware on endpoints
- (vi) Detect compromised credentials & lateral movement
- (vii) Implement 2-factor authentication
- (viii) Train employees on security awareness

⑤ Smishing
1. Smishing & SMS phishing is a technique where a text message is sent to an individual's mobile phone to get him/her divulge personal information.
2. The two most common types of smishing attack are given below:

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

① A person receives a text message that directs him/her to call a phone number to confirm personal or account information

② A person receives a text message that directs him/her to visit a website to confirm the information but is served with a malicious trojan on his/her computer or mobile phone capable of stealing passwords.

③ Organisations should monitor their own SMS number services via sites like whocallsme.com to see if users are suspicious of their services. Such suspicions could indicate mistrust in the legitimate service or attackers who are spoofing the numbers of affected organisation to improve their chances of gaining trust.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q3(b)	What is E-commerce? Explain different types of e-commerce with suitable examples.

E-commerce, also known as electronic commerce, in the simplest form can be defined as buying & selling of goods, products or services over the Internet. E-commerce provides many advantages, however one needs to ensure that the transactions made online are done securely & with genuine parties.

Types of E-commerce

The e-commerce applications, which enable online commercial or sales transactions, can be of different nature.

(A) Business - to - Consumer (B2C)

(1) This category of e-commerce is related to the transactions between a business & the consumer through online shopping portals where details of the products / service displayed.

An example would be a consumer buying a product from an online shopping store like Amazon.com, Flipkart.com, etc.

(B) Business - to - Business (B2B)

(1) The E-commerce transactions belonging

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

to this category are done between two business organisations.
An example, would be of a manufacturer procuring raw material from the seller online, typically, a wholesaler either directly or through a platform like IndiaMART.com.

@ Consumer-to-Consumer (C2C)

The electronic transactions of products or services, in this category are done between two end consumers.
A third party, usually provides an online platform for consumers to identify, & buy or sell, products or services
The most common example for this category would be a platform like eBay.com or olx.in for buying or selling used goods online.

@ Consumer-to-Business (C2B)

The electronic transaction in which an individual consumer provides a service or a good to business & get paid for it.
Typically, an example for this category would be where the consumer

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

can take an online survey on websites like Surveymonkey.com, take freelancing jobs on websites like Freelancer.com, etc for business

© Government-to-Citizen (G2C)

① This model enables the implementation of e-governance, where the citizens can interact with government bodies through the electronic medium & avail services through government websites directly. The examples would include paying of taxes online, registration for birth, marriage & death certificates, participating in government auctions & more.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q4	What is Bluetooth hacking? Explain Bluetooth hacking tools in brief.

① Bluetooth is one of those technologies that is so common that it has become a part of our daily lives.
② It has become a solution to problems like driving & talking on cell phone & introduced new & interesting marketing opportunities for attacks.
③ Bluetooth devices are connected through a process called pairing.
④ One pairing is done, devices bond with one another.
⑤ With the widespread adoption & convenience of Bluetooth devices comes the inevitable implementation problems that cause unexpected things to happen.
⑥ As with most attacks, the first thing to do is to find the device.
This allows legitimate users to find the device they are seeking, but also allows nearby attacker to find those same devices & silently interrogate them to find out if they are suitable to attacks.
⑦ Bluetooth hacking tools are listed as follows:-

① Blue Scanner
This tool enables to search for Bluetooth

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

enable device & will try to extract as much information as possible for each newly discoverable device after connecting it with target.

④ **BlueDriff**

This is a GUI based utility for finding discoverable & hidden Bluetooth-enabled devices.

⑤ **BlueBugger**

The buggers exploit the vulnerability of the device & access the images, phone-books, messages & other personal information.

⑥ **Bluesnarfer**

If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner & to gain access to restricted portions of the stored data.

⑦ **BlueDiving.**

BlueDiving is testing Bluetooth penetration. It implements attacks like Bluebug & BlueSnarf.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q.4(b)	How the Indian penal code IPC 1860 addresses cybercrime?

① The Indian Penal Code (IPC) drafted in 1860, is the official criminal code of India. It provides a general penal code for India & is applicable throughout India, except for the state of Jammu & Kashmir. It contains 23 chapters with 511 sections.

② The Information Technology Act 2000, has several ammendments to the Indian Penal Code.

③ Sections of Indian Penal Code for Cybercrime cases.

Offence	Section of IPC
① Offences by/against Public servant	162, 172, 173, 175
② False electronic evidence	193
③ Destruction of electronic evidence	204, 477
④ Forgery	463 to 477A
⑤ Criminal Breach of Trust	405 to 409
⑥ Counterfeiting Property Mark	482 to 485
⑦ Tampering	489
⑧ Counterfeiting Currency / Stamps	489A to 489E

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

① Section - 29A : Electronic record.

The most important ammendment of the Indian Penal Code by Information Technology Act 2000, is the substitution of the word "document" for the words "document or electronic record". This has brought many cybercrimes directly under the scope of Indian Penal Code related to electronic records.

② Section 463 : Forgery.

Forgery means making of any false document or false electronic record, or part of document or an electronic record. According to the section, a person commits forgery if he/she intentionally makes a false document or a false electronic record, or a part of a document or ~~data~~ cause damage or injury to the public or to any person or to support any claim or title or to cause any person to part with property or to enter into any express or implied contract.

③ Section 464 : Making a false document.

Section 464 of Indian penal code explain meaning of making false document

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

① Dishonestly or fraudly ② makes sign, seals or executes a document or part of document ③ makes or transmits electronic record or part of electronic record ④ affixes any electronic signature, makes any mark denoting the execution of a document.

② Dishonestly or fraudly, without lawful authority, alters a document or an electronic record, which has been executed or affixed with electronic signature either by any person.

③ Dishonestly or fraudly, causes any person to sign, seal, execute or alter a document, or an electronic record or to affix, his/her electronic signature on any electronic record without his/her knowledge, or if that person is of unsound mind or intoxicated, or by deceiving the person about the contents of the documents or electronic record or nature of alteration

④ Section 499 : Defamation

Cyber defamation is done by publishing defamatory material using computers &/or Internet. It includes a defamatory

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

statement about someone on platform like social networking websites, forums or any other electronic channel where people can post content.
The law of defamation under section 499, got extended to "speech" & "Documents" in the electronic form with enactment of ITA, 2000. The offense of defamation is punishable under section 500 of IPC with imprisonment up to two years or fine or both.

Section 500: Punishment for defamation.
Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q.5 (a)	Discuss basic security precautions to be taken to safeguard Laptops & wireless devices.

① To reduce the risk & impact of data loss, organisations must proactively secure confidential data before the laptop or wireless devices are stolen or goes missing

② Some of the basic security principles that need to be followed for laptops & wireless devices are given as follows;

① Choose a secure operating system & lock it down.

- To care about your data, you must pick an OS that is secure.
- Windows 2000 Professional & Windows XP professional both offer secure login, file level security & ability to encrypt data

② Enable a strong BIOS password.

- Security begins right from start by password protecting the BIOS.
- You should find out from your laptop manufacturer what is the procedure for resetting the BIOS password.
- Also find out if the BIOS password locks the hard drive so that it cannot be removed & reinstalled into

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

similar machine.

③ Engrave the laptop

- Permanently marking the outer case of the laptop with your company name, address & phone number may greatly increase your odds of getting it returned to you, if you carelessly leave it in a hotel room or somewhere else.

④ Register the laptop with the manufacturer.

- Registering your laptop with the manufacturer will "flag" it if a thief ever sends it in for maintenance & increases your chances of getting it back.
- It also pays to write down your laptop's serial number & store it in a safe place.

⑤ Get a cable lock & use it.

- Over 80% of laptops in the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm.
- These devices are not very costly &

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

can be found at office supply stores or online
- Tubular locks are preferable to common tumbler lock designs.

⑥ Use a docking station
- Poorly screened housekeeping staff, contractors, & disgruntled employees are the usual suspects.
- You can help prevent this by using a docking station that is permanently affixed to your desktop & has a feature which locks the laptop securely in place.

⑦ Lock up your PCMCIA cards :-
- You can keep someone from stealing the PCMCIA NIC cards or modem that is sticking out of the side of your machine.
- When not in use, eject these cards from the laptop bay & lock them in a safe place.

⑧ Use a personal firewall on your laptop :-
- It is a popular practice for the corporate networks to protect their

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

servers & workstations by configuring a firewall to prevent intruders from hacking their systems via the corporate Internet connection.
- Personal firewalls such as Blackice, ZoneAlarm are an inexpensive & effective layer of security that takes only a few minutes to install must also be used when out of office.

⑨ Use tracking software to have your laptop call home:-
- There are several vendors that offer stealthy software solutions that enable your laptop to check in to a tracking centre periodically using a traceable signal.
- CompuTrace, Secure IT, Stealth signal, & ZTrace provide tracking services for corporations & individuals.

Q.5⑥ What is E-contract? Discuss E-contract Act 1872.

① Internet has significantly changed the way individuals & business communicate & exchange data.
② Trade has increased tremendously between individuals, business organisations

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

of the governments beyond geographic boundaries.

③ With e-commerce, goods & services can be procured & the payment can be made in seconds, increasing the speed, convenience & efficiency of whole process.

④ Traders from two different geographic regions will face delay & difficulty in signing a physical contract, whereas an e-contract can be signed instantly online by both the parties. This saves time & cost as well.

⑤ Many countries have enacted laws to recognise electronic contracts, as the conventional laws relating to contracts is not sufficient to address all issues that arise in electronic contracts.

⑥ In India, the ITA 2000 & the Indian Contract Act 1872, together are used to solve the issues that arise in the formation & authentication of e-contracts.

⑦ An e-contract is legally binding only if it complies with both the laws.

* Types of Electronic Contracts.

① Shrink Wrap Contracts
② Click Wrap Contracts
③ Browse Wrap contracts

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

India Contract Act, 1872

① The Indian Contract Act 1872, defines the term "Contract" under section 2(h) as "An agreement enforceable by law"

② The Act governs the manner in which contracts are made & executed in India.

③ It provides framework of rules & regulations which govern the formation & performance of the contract.

④ The rights & duties of parties entering into the contract & their terms of agreement are decided by the parties themselves.

⑤ The keyword, expressions & their meaning, related to a contract, used in Indian Contract Act 1872 are given below:

Key terms	Section	Definition.
① Offer.	2(a)	When one person signifies to another his/her willingness to do or to obtain from doing anywhere anything, with a view to obtaining the assent of that other

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE		
				to such act or abstinence, he/she is said to make a proposal.
		② Acceptance	2(b)	When a person to whom the proposal is made, signifies his/her assent thereto, the proposal is said to be accepted.
		③ Promise	2(b)	A proposal (Offer) when accepted becomes a promise.
		④ Promisor & Promisee	2(c)	When the proposal is accepted, the person making the proposal is called as promisor & the person accepting the proposal is called as promisee
		⑤ Consider-ation	2(d)	When a desired of the promisor, the promisee or any other person has done or abstained from doing or does or abstains from doing or promises to do or.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE		
				abstain from doing something such act or abstinence or promise is called a consideration for the promise.
		⑥ Agreement	2(e)	Every promise & set of promises forming the consideration for each other
		⑦ Reciprocal Promises	2(f)	Promises which form the consideration or part of it for each other are called reciprocal promises.
		⑧ Void agreement	2(g)	An agreement not enforceable by law is said to be void
		⑨ Contract	2(h)	An agreement enforceable by law is a contract.
		⑩ Void contract.	2(j)	A contract which ceases to be enforceable by law becomes void when ceases to be enforceable
		⑪ Voidable contract	2(i)	An agreement which is enforceable by law at option of 1 or more parties but not at option of other. or others, is a voidable contract

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q.6	Write short note on (Any 2):
	①	Computer Sabotage.

① Sabotage can be defined as a deliberate & malicious act that results in the disruption of normal processes & functions or destruction or damage of equipment or information.

② Computer sabotage involves deliberate attacks intended to disable computers & networks for the purpose of disrupting commerce, education & recreation for personal gain, committing espionage, or facilitating criminal conspiracies, such as drugs & human trafficking.

③ According to the Federal Bureau of Investigation, it costs billions of dollars in legal fees to recover damages such as identity theft & to repair vital infrastructure that serves hospitals, banks & 911 services.

④ Committing computer sabotage can be as simple as deliberately infecting a computer with a virus to keep authorized users from logging in.

⑤ Although not always, much computer sabotage involves the use of malware such as bots, worms, viruses & other spyware, which enables hackers to gain

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

START WRITING HERE

Space for Marks	Question No.

illegal access to personal & corporate computers.

⑥ Protecting from computer sabotage means taking proactive measures to guard hardware & software.

⑦ Besides installing & maintaining a firewall & antivirus software, establish separate user IDs for each person who uses a computer.

⑧ Never post list of usernames & passwords & take the time to change passwords as soon as account shows signs of having tampered with.

⑨ When using a public, school or workplace computer, always report logs & aberrant performance to alert support staff that the system may have been compromised.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	②	Indian Information Technology Act, 2000 ① The Indian Information Technology Act, 2000 is also known as ITA 2000, or IT Act. ② It is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It became the primary law in India to deal with cyber crime & electronic commerce. ③ The Indian IT Act, 2000 is based on the Model law on e-commerce & with its adoption, India became the twelfth country to enable cyberlaw. • Objectives of the ITA 2000 ① The IT Act 2000, provides legal recognition to the transactions done using electronic data interchange & other electronic means of communication or electronic commerce transactions, which may involve the use of alternatives to a paper-based method of communication & information storage to facilitate the electronic filing of document with government agencies. ② The Act further amends the following existing laws - the India Penal code 1860, the Indian Evidence Act 1872, the Banker's Books Evidence Act 1891 &

Total Marks of Question no.		Examiner
		Moderator
		Re-Assessor

START WRITING HERE

Space for Marks	Question No.

the Reserve Bank of India Act 1934.

• Features of Information Technology Act 2000.

Some of the prominent features are listed:-

① It provides legal recognition to records in electronic form.

② It provides legal recognition to e-commerce & electronic transaction in India.

③ It provides legal recognition to digital signatures issued & authenticated by certifying Authorities.

④ It is applicable to cybercrimes & contraventions committed in India & outside India by any person, irrespective of nationality, if the cybercrime is committed in India or involved any computer based in India.

⑤ It has appointment adjudicating officers for holding inquiries under the Act.

⑥ It elaborates on offences, penalties & breaches.

⑦ It has established the Cyber Appellate Tribunal to hear appeals.

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

③ Write key IT requirements for SOX & HIPAA

(A) SOX

① Sarbanes - Oxley Act of 2002 is also commonly known as Sarbanes Oxley, Sarbox or SOX.

② It is also called the "Public Company Accounting Reform & Investor Protection Act" & the "Corporate & Auditing Accountability, Responsibility & Transparency Act".

- **Key IT Requirements : SOX**

① There must be a written security policy in the company.

② The company should baseline its current compliance state & be prepared to show progress towards full compliance. SOX is commonly applied with progressive requirements year over year.

③ Additional sections of SOX require "timely monitoring & response" to issues that may materially affect data used or relied upon to generate public financial reports.

In IT terms - you need to monitor your logs, & responds to threats. SIEM tools & Intrusion Detection / Prevention Systems are commonly

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

inferred from "timely monitoring"

④ The company must log & audit access to financial data & critical files used in the preparation of public financial reports.

⑧ HIPAA

① The Health Insurance Portability & Accountability Act of 1996 is also called the Kennedy-Kassebaum Act.

② It was created to modernise the flow of healthcare information & stipulate a way in which the Personally Identifiable Information could be maintained by the healthcare & healthcare insurance sector.

• Key IT Requirement : HIPAA

Organizations need to

① Conduct an initial risk assessment, periodic reviews & reassessments

② Designate security person.

③ Implement termination policy & procedures.

④ Have a written security & incident handling policy

⑤ Have a back-up, emergency operation & disaster recovery plan

⑥ Have policies for the use of the Internet, various systems & reusable

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Storage media along with their reuse & disposal plan.

⑦ Have audit controls, including unique user identifiers, for authentic users, recording & auditing user sessions & logout / disconnect inactive sessions.

⑧ Have a policy to encrypt sensitive data, monitor & audit access & alterations to sensitive data, protect data in transmission with backup.