Case Study 1

- Xgen Networks Pvt Ltd provides Internet services to Robust Software solutions.
- Robust Software cleared all its monthly bills.
- Xgen had some billing issue and they barred the internet services to Robust Software despite repeated reminders from Robust that their bills were paid.
- Robust Software suffered tremendous loss due to the disrupted Internet Services.
- What would you suggest Robust Software?

shivam387@yahoo.com

Sec 65 : Tampering with Computer Source documents.

Punishment – Imprisonment upto three years or fine upto Rs 2 Lacs or both.

Sec 66 : Penalises any contravention u/s 43 if carried out with a fraudulent or dishonest motive

Punishment – Imprisonment upto three years or fine upto Rs 5 Lacs or both.

Sec 66 A : Punishment for sending offensive messages through communication service etc...

Requisites : offensive or menacing or false, or for the purpose of annoyance, inconvenience, ill will etc...

Punishment – Imprisonment upto three years and with fine.

shivam387@yahoo.com

- Sec 66 B : Punishment for dishonestly receiving stolen computer/resource etc.
- Sec 66 C : Punishes identity theft (DSC, passwords, or such unique identification.)
- Sec 66 D : Punishes personating, by means of Computer resource.
- Sec 66 E : Punishes violation of privacy rights.
- Sec 66 F : Punishes Cyber Terrorism

shivam387@yahoo.com

Sec 67A : Punishment for publishing or transmitting of material containing sexually explicit act, etc.. In the electronic form.

Punishment :

1st conviction-Imprisonment upto 5 years and fine upto Rs 10 Lacs.

2nd conviction-Imprisonment upto 7 years and fine upto Rs 10 Lacs.

EXCEPTION

Art, Science, literature or other interests of learning and other cases

Sec 67B : Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc.. In the electronic form. (Readwith other sub rules)

Punishment :

1st conviction-Imprisonment upto 5 years and fine upto Rs 10 Lacs.

2nd conviction-Imprisonment upto 7 years and fine upto Rs 10 Lacs.

Sec 67C : Preservation & retention of information by intermediaries.

Punishment - Imprisonment upto three years and with fine.

shivam387@yahoo.com

- Sec 68 : Provision and punishment for violation of orders from the Controller.

- Sec 69 : Powers of the Govt. to issue direction for monitoring, intercepting or decrypting any information through any Computer Resource.

(Basically an administrative right of the Govt. and provides for punishment to the violator, usually intermediaries who are incharge of such database or are service providers.)

Sec 69 A powers for blocking of public access

Sec 69 B power to authorize monitor and collect traffic.

shivam387@yahoo.com

- Sec 71 : Penalty for Misrepresentation before Controller or the Certifying Authority
  - Punishment - Imprisonment upto 2 years or fine upto Rs. 1 Lac or both.

- Sec 72 : Penalty for breach of Confidentiality & privacy, the provision applies to those persons who are empowered under this Act with such a database or records.
  - Punishment - Imprisonment upto 2 years or fine upto Rs. 1 Lac or both.

- Sec 72A : Penalty for disclosure of information in breach of Lawful Contract –(an amendment to include even the employees of private organisations or such intermediaries working therein)
  - Punishment - Imprisonment upto 3 years or fine upto Rs. 5 Lac or both.

shivam387@yahoo.com

- Sec 74 : Publication of Signature or signatu certificates for fraudulent purpose.
  - Punishment - Imprisonment upto 2 years or fine upto Rs. 1 Lac or both.

- Sec 76 : provides for confiscation of any related computer accessory, system part etc if the same is believed to be used in any violation of this Act or rules.

shivam387@yahoo.com

- Sec 77 B : Offences punishable with imprisonment upto 3 years to be bailable.

- Sec 78 : Power to investigate offences now available to Inspector, earlier the onus was on the DSP rank officer or above.

shivam387@yahoo.com

- Sec 79 : Exemption of Intermediaries and service providers if they establish that they have exercised due diligence on their part.

- An abusive provision for the ISP's but often helpful !

shivam387@yahoo.com

- The 2009 notification makes it an offence to even abet or attempt a cyber crime, earlier unsuccessful criminals always escaped by virtue of this grey area.

- Sec 84 B : Punishment for Abetment
  - Same punishment as prescribed for the offence

- Sec 84 C :Punishment for attempt
  - A maximum of one-half of the term of imprisonment provided for the offence, or with fine as prescribed for the offence or with both.

- Sec 90: State Govt. has powers to make allied rules.

shivam387@yahoo.com

The Indian Penal Code
Vis-à-vis
The Cyber Crime

shivam387@yahoo.com

Relevant application of IPC etc…

Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forging electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Online sale of Drugs	NDPS Act
Web - Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

The Evidence Act

- Filing an FIR is easy, but not chargesheet.
- Digital evidence is extremely volatile & difficult to preserve.
- Indian criminal justice system requires guilt to be proved beyond reasonable doubt.

shivam387@yahoo.com

Evidence Act

- The major highlight of the Evidence Act in view of the IT Act 2000 is that it recognises electronic evidence.
- Sec 65 is the most important provision dealing with specific provision on digital evidence.
- Sec 65B provides for a detailed process for the analysis of the digital evidence in question.
- Sec 65 B (4) requires a certificate from the examiner of digital evidence.

shivam387@yahoo.com

Evidence Act

- The Govt. shall notify who is the gazetted examiner for Digital evidence u/s 79 A of the IT Act.

- The same provision is exclusive, it excludes all other Cyber Forensic experts from entering this field u/s 45 of the Evidence Act.

shivam387@yahoo.com

Is digital evidence binding upon courts ?

- Is EnCase/FTK approved by Central govt. for this purpose?
- Is e-mail/sms admissible as evidence?
- Is data retrieved from remote servers acceptable?

shivam387@yahoo.com

- Is EnCase/FTK approved by Central govt. for this purpose?

Answer : It is not required, the testimony of such an evidence is viewed as a mere opinion of the expert. Do not be confused for NIST(USA) Policy, although a standard approval should help.

shivam387@yahoo.com

Detrailing tricks !

- Keep altering the time clock.
- Keep the PC infected with viruses and Trojans.
- Use (Kernel)modified forms of OS.
- Use unknown applications.
- Keep the PC in defective mode.
- Use hardware that is difficult to find.

- *Never try any trick which directly co-relates with an attempt to destroy evidence.*

shivam387@yahoo.com

Need of the hour ?

- To strengthen investigation mechanism by making it a quick response cell.
- Educate the IO's, about handling & processing, search & seizure.
- Advanced Lab with skilled personnel.
- YOU HAVE TO join hands with IT Professionals.
- Keep upgrading.
- Remember, It's a white collar crime.

shivam387@yahoo.com

Law is
the last interpretation of the law,
given by the last judge.

-Anonymous

shivam387@yahoo.com

Thank you

shivam387@yahoo.com

94339 22172