

INTRODUCTION

What is a role
of IS
professional?

- To manage liability for privacy
- Security Risks
- Reduce risks from Electronic and Physical Threats

What they
should
understand?

- understand the current legal environment
- stay current with laws and regulations
- watch for new and emerging issues

How they
Can?

- By educating management and employees
- Proper use of Information security

LAWS AND ETHICS IN INFORMATION SECURITY

- Laws
 - Rules that mandate or prohibit certain behavior
- Ethics
 - Define socially acceptable behaviors
- Key difference
 - Laws carry the authority of a governing body
 - Ethics do not carry the authority of a governing body
 - Based on cultural mores
 - Fixed moral attitudes or customs
 - Some ethics standards are universal

ORGANISATIONAL LIABILITY AND THE NEED FOR COUNSEL

- What if an organization does not demand or even encourage strong ethical behaviour from its employees?
- What if an organization does not behave ethically?
- Even if there is no breach of criminal law, there can still be liability.
- **Liability** is the legal obligation of an entity that extends beyond criminal or contract law;
- It includes the legal obligation to make restitution, or to compensate for wrongs committed

ORGANISATIONAL LIABILITY AND THE NEED FOR COUNSEL

- The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action.
- An organization increases its liability if it refuses to take measures known as due care.
- **Due care** standards are met
 - when an organization makes sure that every employee knows what is acceptable or unacceptable behavior,
 - knows the consequences of illegal or unethical actions.

ORGANISATIONAL LIABILITY AND THE NEED FOR COUNSEL

- **Due diligence** requires

- an organization make a valid effort to protect others and continually maintains this level of effort.

- **Long arm jurisdiction—**

- the long arm of the law extending across the country or around the world to draw an accused individual into its court systems.

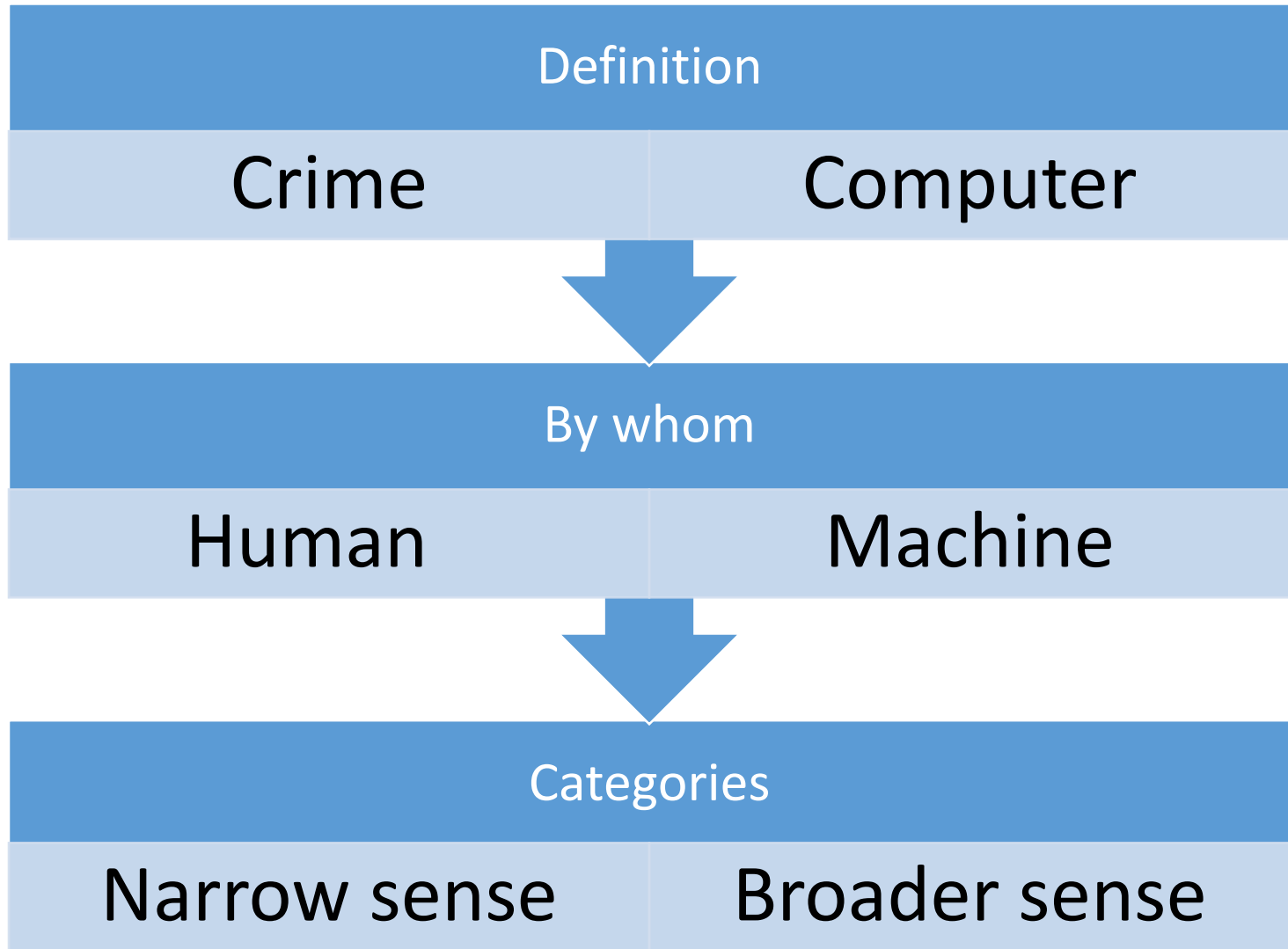
POLICY VERSUS LAW

- Policies
 - Guidelines that describe acceptable and unacceptable employee behaviors.
 - Functions as organizational laws.
 - Has penalties, judicial practices, and sanctions.
- Difference between policy and law-
 - Ignorance of policy is acceptable.
 - Ignorance of law is unacceptable.

POLICY VERSUS LAW

- Keys for a policy to be enforceable
 - Dissemination- Distributed to all individuals who are expected to comply with them.
 - Review- Readily available for employee reference
 - Comprehension- Easily understood, with multilingual, visually impaired and low- literacy translations.
 - Compliance- Acknowledged by employee with consent form.
 - Uniform enforcement- Enforced for all employees, regardless their status or assignment.

What is Cyber Crime ?



Cyber Frauds in India

- As per report



1,15000
people
(everyday)

80 per minute
(one per
second)

Average
financial
10500

Classification of Cyber Crimes

- Tampering with computer source documents
- Hacking
- Publishing of information, which is obscene in electronic form
- Accessing protected system
- Breach of confidentiality and privacy

Types of Cyber crime

- **Cyber Stalking**
- **Cyber squatting**
- **Data Diddling**
- **Cyber Defamation**
- **Trojan Attack**
- **Forgery**
- **Web Jacking**
- **Financial crimes**
- **Internet time theft**
- **Virus/worm attack**
- **E-mail spoofing**
- **Email bombing**
- **Salami attack**

CYBER CRIMES FOUND IN INDIA

- **Sale of illegal articles**
- **Online gambling**
- **Intellectual Property crimes**
- **Email spoofing**
- **Unauthorized access to computer systems or networks**
- **Email bombing**
- **Salami attacks**
- **Trojan Attack**
- **. Cyber stalking**

WHO COMMITS CYBER CRIME?

- Insider
- Hacker
- Virus writer
- Foreign intelligence
- Terrorists

CYBER CRIME ON THE RISE

- As per the cyber crime data maintained by the National Crime Records Bureau (NCRB)


INFORMATION TECHNOLOGY ACT,2000	2007	2008	2009	2010
CASES FILED	217	288	420	966
ARRESTED	154	178	288	799

C YBER CRIME, INDIAN PENEL CODE (IPC)	2007	2008	2009	2010
CASES FILED	328	176	276	356
ARRESTED	429	195	263	294

Cyber Crime on the rise

WHAT KEEPS **CYBER COPS** ON TOES

Cyber Crime	2017 (till Oct)	2016
Online banking	2,095	1,343
FB-related	316	151
Email hacking	125	97
Sexual harassment	81	51
Lottery fraud	42	15
Data theft	47	43
Job fraud	49	40
Twitter-related	12	4
Total cases	3,474	2,402



CYBER LAW OF INDIA

- In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000.
- The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.
- The following Act, Rules and Regulations are covered under cyber laws:
 1. Information Technology Act, 2000
 2. Information Technology (Certifying Authorities) Rules, 2000
 3. Information Technology (Security Procedure) Rules, 2004
 4. Information Technology (Certifying Authority) Regulations, 2001

INFORMATION TECHNOLOGY ACTS

- *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model)
- signed by President [K. R. Narayanan](#) on 9 May 2000. finalised by [Pramod Mahajan](#)

Section	Offence	Description	Penalty
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	Imprisonment up to three years, with fine.

Sl.No	Offences	Section Under IT Act
1.	Tampering with computer source Documents	Sec.65
2.	Hacking with computer systems , Data Alteration	Sec.66
3.	Sending offensive messages through communication service, etc	Sec.66A
4.	Dishonestly receiving stolen computer resource or communication device	Sec.66B
5.	Identity theft	Sec.66C
6.	Cheating by personation by using computer resource	Sec.66D
7.	Violation of privacy	Sec.66E
8.	Cyber terrorism	Sec.66F
9.	Publishing or transmitting obscene material in electronic form	Sec .67
10.	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec.67A
11.	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Sec.67B
11.	Preservation and Retention of information by intermediaries	Sec.67C
12.	Powers to issue directions for interception or monitoring or decryption of any information through any computer resource	Sec.69
13.	Power to issue directions for blocking for public access of any information through any computer resource	Sec.69A
14.	Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security	Sec.69B
15.	Un-authorized access to protected system	Sec.70
16.	Penalty for misrepresentation	Sec.71
17.	Breach of confidentiality and privacy	Sec.72
18.	Publishing False digital signature certificates	Sec.73
19.	Publication for fraudulent purpose	Sec.74
29.	Act to apply for offence or contraventions committed outside India	Sec.75
21.	Compensation, penalties or confiscation not to interfere with other punishment	Sec.77
22.	Compounding of Offences	Sec.77A
23.	Offences with three years imprisonment to be cognizable	Sec.77B
24.	Exemption from liability of intermediary in certain cases	Sec.79
25.	Punishment for abetment of offences	Sec.84B
26.	Punishment for attempt to commit offences	Sec.84C
27.	Offences by Companies	Sec.85
Note : Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act		
28.	Sending threatening messages by e-mail	Sec .503 IPC
29.	Word, gesture or act intended to insult the modesty of a woman	Sec.509 IPC
30.	Sending defamatory messages by e-mail	Sec .499 IPC
31.	Bogus websites , Cyber Frauds	Sec .420 IPC
32.	E-mail Spoofing	Sec .463 IPC
33.	Making a false document	Sec.464 IPC
34.	Forgery for purpose of cheating	Sec.468 IPC

36.	Web-Jacking	Sec .383 IPC
37.	E-mail Abuse	Sec .500 IPC
38.	Punishment for criminal intimidation	Sec.506 IPC
39.	Criminal intimidation by an anonymous communication	Sec.507 IPC
40.	When copyright infringed:- Copyright in a work shall be deemed to be infringed	Sec.51
41.	Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of	Sec.63
42.	Enhanced penalty on second and subsequent convictions	Sec.63A
43.	Knowing use of infringing copy of computer programme to be an offence	Sec.63B
44.	Obscenity	Sec. 292 IPC
45.	Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail	Sec.292A IPC
46.	Sale, etc., of obscene objects to young person	Sec .293 IPC
47.	Obscene acts and songs	Sec.294 IPC
48.	Theft of Computer Hardware	Sec. 378
49.	Punishment for theft	Sec.379
50.	Online Sale of Drugs	NDPS Act
51.	Online Sale of Arms	Arms Act

Continued

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Amendment Act 2008

- Focussing on data privacy
- Focussing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like cyber terrorism
- authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

NEED FOR CYBER LAW IN INDIA

- First the coming of the Internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of Cyber laws.
- Secondly, the existing laws of India, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace.
- Thirdly, none of the existing laws gave any legal validity or sanction to the activities in Cyberspace.
- Fourthly, Internet requires an enabling and supportive legal infrastructure in tune with the times

NEED FOR CYBER LAW IN INDIA

- Almost all transactions in shares are in demat form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.

- Even in "non-cyber crime" cases, important evidence is found in computers / cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
- Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business

CASE

- In November 2012, IPS officer Amitabh Thakur and his wife social activist Nutan Thakur, filed a petition in the [Lucknow](#) bench of the [Allahabad High Court](#) claiming that the Section 66A violated the freedom of speech guaranteed in the Article 19(1)(a) of the [Constitution of India](#). They said that the section was vague and frequently misused.^[24]
- Also in November 2012, a Delhi-based law student, [Shreya Singhal](#), filed a [Public Interest Litigation](#) (PIL) in the Supreme Court of India. She argued that the Section 66A was vaguely phrased, as result it violated Article 14, 19 (1)(a) and Article 21 of the Constitution. The PIL was accepted on 29 November 2012.^{[25][26]} A similar petition was also filed by the founder of [MouthShut.com](#), [Faisal Farooqui](#),^[27] and NGO Common Cause represented by [Prashant Bhushan](#).^[28] In August 2014, the Supreme Court asked the central government to respond to petitions filed by [Mouthshut.com](#) and later petition filed by the [Internet and Mobile Association of India](#) (IAMAI) which claimed that the IT Act gave the government power to arbitrarily remove user-generated content.