INNOVATIONS IN TEACHING & LEARNING PROCESS TO ENHANCE E-LEARNING IN NURSING EDUCATION

Dr. Anupama Vinay Oka
Associate Professor, Obstetrics & Gynaecology
KDA Nursing College Mumbai, India
Email: dranupamaoka@gmail.com

ABSTRACT

As observed and experienced, most of the organizations especially related with the IT / ITES sectors and those having multi-national transactions have their Information Security teams in place. The conventional methods are no more used as every day something new crops up in this fast changing sector. But there are three major questions that arise and are a common factor which most of the organizations ask their ‘Trusted’ Systems Administrators.

1. How to prevent the attacks on the computer systems and safeguard the confidentiality of the organizational data.

2. Are the Systems Department or the Network Security Teams capable of detecting System attacks by different external agents like computer viruses, worms, Trojans etc.

3. Is the organization having the capability to provide adequate and timely response to such attacks and provide solutions so as to prevent future attacks?

The Systems Administrator and the Network Security team in any organization-including Educational Institutions, normally have to provide to each individual employee a User Name and Operational Password. With this in place the Systems personnel should provide each employee with accountable access restricted to their area or scope of operations. The security parameters should include legal notifications, upgradation of existing firewall mechanisms, and periodical assessment of the installations to prevent the attacks on the machines in the organization.

Keywords: Information Security, Network Security, Response, Accountable Access, Firewall Mechanisms

INTRODUCTION

Earlier the Internet usage was only to the privileged class. Now we have mobile internet in the era of globalization, mobile banking, internet banking, online purchases, chatting, access to mails and utility services, it is imperative that our Cyber Law that is: The IT Act is very important for every Indian as the law of the land of this country. E-mails, mobile communication, transactions have been convenient by the use of such devices and services. Though there are advantages, so are the disadvantages. In order to know the differences and the provisions, it is equally important for us that this law concerns us Indians as this is the law of our country. So we have to draw logical conclusions on the utility and how best we prevent ourselves from being victims of Cyber Crimes.

Study of the legal angles, especially our Indian IT Act of 2000, with the amendments of 2008, the Law of our land is important in a way because any transaction on the internet from our land is binding on us. This Act touches all the important aspects right from the communication devices, the networks and

Available online on www.abhinavjournal.com
the applicable sections along with it the implications of the violations are important for us as part of education and a part of academic curriculum in Post Graduate education programs. Initially it was thought that this act and its provisions were technical in nature. But after reading the provisions, it is really simplified and applicable to all the users of not only the internet, but also those who use the mobile phones, use the services of service providers as well as the Internet service providers, the peripheral devices like PDAs, Memory Cards, Card Readers, Scanners Cameras all are part and parcel of these utility devices. Learning about all these is equally important for a common man and imparting education to school students, college students, working people as well as anybody who uses such devices. The educationists should device a plan to spread the awareness on these issues to the common man in public interest.

When any user goes online for making any financial transaction for example online purchase: The basic question naturally arises should the transaction be made. Or Is the site secure. Are the transactions authentic? So naturally any user of the services; if he is aware of the legal provisions, safety and security of the internet will opt for going online and conclude his transaction.

In academics as well as for the general public, Virtual Marketing has been included as a knowledge disseminating subject and new ways to do business in the era of globalization.

As a part of learning the basics of Information technology and its channels, it is a must to know about the Hardware components of the computer systems, its compatibility and also include the peripheral devices like the scanners, printers, portable drives memory cards etc. The Software components which include the Operating Systems, Antivirus software, and the Connectivity of the services through the Internet. and the protection of our complete system including the data and our transactions. Transacting on the Internet has wide legal implications as it alters the conventional methods of doing business. To build enduring relationships with online customers the legal issues of e-transactions need to be addressed from the onset.

From education point of view, since subjects like Virtual Marketing, Fundamentals of IT, IT for Management, MIS are there in Post Graduat e Management Programs focus should also be given on the Cyber Law Awareness Program.

As the popularity and usage of internet services grew, the service providers and the users had not imagined the scope of the activities in relations to its use and misuse. Laws varied from country to country and there was limited scope on the applicability of the laws. A cybercrime committed in India was not necessarily a crime in any other country. Therefore a control on these kinds of activities required a strict vigil with the help of strong regulations and regulatory bodies. Internet services are the need of the hour for faster communication today and most of the organizations are using it as the most popular media of communication, many positive as well as negative events taking place world-wide. Criminalization of Internet usage is on the rise due to its borderless medium, there is a strong need for application of cyber laws in India to control such cybercrimes.

India is one of the few countries in the world to have its own separate ordinance related with Information technology.

Crime Perpetrator

A Person who is relatively young (under 30 years of age), highly motivated, Intelligent, adventurous, maybe a good worker, having no previous criminal record, maybe unhappy with job, maybe employed for several years on the same post, in the same place, possibly over qualified for current position, egoistic, and sometimes feels exploited, and may want compensation.

But if we see the current scenario, the crime base is shifting from Computer Based Crime to Mobile Phone Crimes. The rampant use of ‘Apps’ is aiding the Mobile phone user to go for internet services on these communication devices and are using the same on Tablets, handsets supporting features like What app, Google maps, and those which can give or provide data on finger tips. Ongoing war between Android as well as Windows based Handsets can be seen through advertisements on the
electronic as well as in the print media. Popularity shows that monopoly business may not last long and consumers/users may require options in operations. Likewise consumer demand and market shift displays the trend more from the B2B aspect to the B2C aspects which would prove its results over the coming days.

Table: Country Specific Legislative Response to Cybercrime

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Country</th>
<th>Legislative Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Australia</td>
<td>Cybercrime Act, 2001, amending existing laws that have bearing on cybercrime.</td>
</tr>
<tr>
<td>2</td>
<td>Austria</td>
<td>Protection of personal Data (the Privacy Act), 2000, A comprehensive legislation in the field of protection of privacy in cyber space.</td>
</tr>
<tr>
<td>3</td>
<td>Belgium</td>
<td>The Belgian Criminal Code was amended in November 2000 and provisions were made to incorporate computer forgery, computer fraud, hacking and sabotage as criminal offences under the law.</td>
</tr>
<tr>
<td>5</td>
<td>Estonia</td>
<td>Estonian Criminal Code contains provisions on certain types of cyber crimes.</td>
</tr>
<tr>
<td>6</td>
<td>Germany</td>
<td>Provisions included in German Penal Code on certain cyber-crimes. Other provisions in the Code applicable to crimes committed through the help of medium of computer or computer networks.</td>
</tr>
<tr>
<td>7</td>
<td>Ireland</td>
<td>The Criminal Damage Act, 1991; includes extensive provisions on damages caused to or by a computer system or network.</td>
</tr>
<tr>
<td>8</td>
<td>Malaysia</td>
<td>The Computer Crimes Act, 1997; deals exclusively with computer crimes.</td>
</tr>
<tr>
<td>9</td>
<td>Malta</td>
<td>The Electronic Commerce Act, 2001; essentially an Act to regulate electronic commerce, its part VII, contains amending provisions with regard to ‘computer misuse’ to be incorporated Criminal Code of the country.</td>
</tr>
<tr>
<td>11</td>
<td>Philippines</td>
<td>The Electronic Commerce Act, 2000; Section 33 prescribes penalties for certain cybercrimes like hacking, cracking, piracy etc.</td>
</tr>
<tr>
<td>12</td>
<td>Romania</td>
<td>According to the Romanian Law, amendment in the Title III of Anti Corruption Law No. 676 on The processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. Law No. 196/2003 on Prevention and fighting of Pornography was added as a criminal offence.</td>
</tr>
</tbody>
</table>
With the changes applicable in the industry, the law related to Information Technology in our country that is The Indian IT Act of 2000, with its amendments made in the year 2000, there has been a considerable shift from computer based crime to Mobile phone based crime. As a preventive and a precautionary measure, the Mobile Phone / Cellular Phone came in the ambit of Communication Device and defined separately under this act.

The modifications or amendments in some of the critical sections of the Act have been listed as under for updated information and interpretations.

As per the records available from the Legal perspectives and Cyber Crime Cell of Pune, as well as the Police Manual of Government of Maharashtra.

I have quoted some of these sections for reader benefits.

These sections have been drawn from the main Act and its amendments.

SECTION 2(1) (i) of the Indian IT Act of 2000, with its amendments of 2008,

“Computer”: The computer is defined as:

“Any electronic magnetic, optical or other high-speed data processing device or system, which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes: input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network”.

After Clause (h), of the Indian IT Act of 2000, with its amendments of 2008, the following clause has been added but never discussed our taught in the classroom despite the Act being included in the Syllabus:

SECTION 2(1) (ha) of the Indian IT Act of 2000, with its amendments of 2008, has clearly defined what a “Communication Device” is.

Communication Device: “It includes cell phones, personal digital assistance devices [PDAs], or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image”.

SECTION 2 (1) (na) of the Indian IT Act of 2000, with its amendments of 2008, has clearly defined the word “Cyber Café”

Cyber Café: “Any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public”.

SECTION 2 (1) (nb) of the Indian IT Act of 2000, with its amendments of 2008, has defined the words “Cyber Security”.

Cyber Security: “Protecting information, equipment, devices, computers, computer resources, communication devices, and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction”.

After Clause (t), the following has been inserted:

SECTION 2 (1) (ta) of the Indian IT Act of 2000, with its amendments of 2008, has modified the meaning and the words from “Digital Signature” to “Electronic Signature”.
Hence for the wherever the word ‘Digital” has been used, it shall be substituted by the word ‘Electronic”. Therefore,

‘Electronic Signature: “Authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes Digital Signature”.

SECTION 2 (1) (tb) of the Indian IT Act of 2000, with its amendments of 2008, has modified the meaning and the words “Digital Signature Certificate” to “Electronic Signature Certificate”

Electronic Signature Certificate: Means “An Electronic Signature Certificate issued under Section 35 and includes Digital Signature Certificate”.

Apart from the above there are other sections which are applicable under the IT Act, 2000, with the Amendments of 2008. The applicability of the Section, with its penalties I have listed below for knowledge enhancement.


The Law reads as:

“If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both”.

“The word ‘dishonestly’ to be interpreted and action under Section 24 of the Indian Penal Code applies”.

“Similarly the word ‘Fraudulently’ to be interpreted and action under Section 25 of the Indian Penal Code applies”.

The latest inclusion and amended with the recent events concerning the arrest and later release of two teenage girls in Mumbai suburbs related with posts on Facebook:


(a) “Any information that is grossly offensive or has menacing character” or

(b) “Any information which he known to be false, but for the purpose of causing annoyance, inconvenience, danger, obstructions, insult, injury, criminal resource” or a “Communication device”.

(c) “Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the address or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine”.

Explanations – For the purpose of this section, terms ‘electronic mail’ and ‘Electronic mail message’ means a message or information created or transmitted or received on a computer, computer system, computer resources or communication device including attachments in text, images, audio video and any other electronic record, which may be transmitted with the message. His also means that E-mail or SMS sent through a communication device may be admissible as evidence in the Court of Law as per the Indian Evidence Act.

But due to the complex nature of this section and its wide ambit, it is necessary for the protectors of law to exercise restraint while applying this section in the society.

Example: The Police Department faced a lot of flak for their high handed approach in the arrest of the teenage girls and being ordered by the Hon’ble court to observe restraint while exercising their powers and duties.
The interpretation and applicability also extends “Provided that provisions of Section 67-A of the Indian IT Act of 2000, with its amendments of 2008, and this section does not extend to any book, pamphlet, paper, writing, drawing painting representation or figure in electronic form” –

1. “The publication of which is provided to be justified as being for the public good on the ground that such book, pamphlet paper writing drawing painting representation or figure is the interest of science, literature art or learning or other objects of general concern”

OR

2. “Which is kept or used for bonafide heritage or religious purposes”.

Explanation – For the purpose of this section ‘Children’ means a person who has not completed the age of 18 years.

This particular clause raises concern on the age factor to describe a MAJOR.

1. The voting right of a person brought down from 21 years to 18 years.
2. Driving License issued at the age of 18 years and above.
3. Liquor License procured at the age of 18 years and above.
4. All crimes committed at the age of 18 and above, punishment as per the severity of the crime applies.
5. A crime like Rape at 17 years and above but under the age of 18, the criminal treated as Juvenile and sent to a correction centre till he attains the age of 18 and let off scot free.

A lot of introspection should be done before such laws are being framed rather than gaining a political mileage for vote bank politics and for political gains which may have a reverse impact on the socio-economic parameters. The law makers should seriously think and act on such matters which have a deep impact on the society which we all see and read on a daily basis but do nothing about it.

CONCLUSION

ADVANTAGES OF Indian IT Act 2000 with its amendments

This Act, the law of our land has provided us a platform for keeping control on the various aspects of cybercrimes resorted to by the criminals who have and are encashing on the loopholes of the act. Electronic Records as well as Electronic Signature Certificates have been given due credence and legalized in India.

The IT Act 2000 with its amendments of 2008 has provided a framework to deal with cybercrimes. Examples have been given herewith to show the applicability of the Act, where it has been successful and for the purposes in which all the provisions have been framed.

The IT Act 2000 with its amendments of 2008 has enabled the government departments to introduce e-governance in a very effective manner in which the government departments now are accepting e-filing of documents like online submissions of taxes, bills, challans, reports and accepting them and retaining such documents in electronic formats. Legal authenticity has been provided to electronically filing of documents and records.

E-mail communication in India has been given authenticity and now is accepted as a valid mode of communication with legal binding and due credence in the court of law. The implication of this valid form of communication is that such e-mails / electronic form of messages or communication can be produced as evidence in the court of law with the additional cover provided by the provisions and applicable sections of The Indian Evidence Act. Legal proceedings can be initiated in such cases as per the provisions and its applicability.
The Act has modified the terms and references related to digital / electronic signatures as well as
digital / electronic signature certificates as per the statutes and provisions in the act.

Breaking into the computer systems or computer networks have been dealt with severity under the
provisions and applicable sections and thereby providing a sense of security to the corporate sector
which such crimes are on the rise. Apart from punishment or conviction, penalties as well as
compensatory measures have been added. Monetary damages have been imposed on the criminals or
perpetrators of such crimes, not exceeding Rs. 1 crore.

Appointment of Controllers, Assistant / Deputy Controllers have been provided in our act.
Appointment of Adjudicating Officers for investigating cybercrimes and the setting up of a Cyber
Regulations Appellate Tribunal [CRAT] has been made in this act.

The law has made provisions and set strict guidelines for Internet Service providers and Licensing
authorities as well as liabilities on providers as well as users.

The IT Act 2000, has tough and strict provisions as laid down in the amendments, but the applicability
and implementation is very difficult as the awareness among the public as well as the authorities is less
and due to such limitations o far even if the crimes have taken place, the conviction ratio has been very
poor in practical situations.

**Disadvantages of Indian IT Act 2000 with its amendments of 2008**

Internet is a borderless medium; it spreads to every corner of the world where life is possible and
hence is the cybercriminal. Then how come is it possible to feel relaxed and secured once this law is
enforced in the entire nation?

The Act initially was supposed to apply to crimes committed all over the world, but nobody knows
how can this be achieved in practice, how to enforce it all over the world at the same time?

The law relies totally on the Intellectual Property Rights Act, as there are no separate provisions under
the IT Act for such violations. The IT Act has only the framework for such penalties and crimes. But
no particular sections under which a person or an organization can be booked for such violations.
There are no provisions covered for copyrighting, trade marking or patenting of electronic information
and data. The law is also silent on the rights and liabilities of domain name holders, the first step of
entering into the e-commerce.

The law is silent on the negotiable instruments from the applicability of the IT Act, as it deals only
with particular transactions and not in its entirety, which may have major effect on the growth of e-
commerce in India. It leads to make the banking and financial sectors irresolute in their stands.

The IT Act stays silent on filming anyone’s personal actions in public and then distributing it
electronically. It holds ISPs (Internet Service Providers) responsible for third party data and
information, unless contravention is committed without their knowledge or unless the ISP has
undertaken due diligence to prevent the contravention.

According to Amendments made in 2008 to the IT Act 2000, now an officer in the rank of Police
Inspector is empowered to look up into the investigations and filling of charge sheet when any case
related to cyber law takes place.

This approach is likely to result in misuse in the context of Corporate India as companies have public
offices in the metros and semi-metro cities, which would come within the ambit of “public place”
under the Act. As a result, these companies will not be able to escape potential harassment at the hands
of the Investigating Officer.

The age factor of 18 years for a major and any one below the age of 18 described as ‘Child’ or
‘Children’ should be thought over carefully and considered while any serious organized crime is being
investigated.
Facebook has reduced the age of its members from 18 years to 13 years without considering the Law or seeking Legal opinion on the reduction of the age group; and its implications in society as the ‘children’ under this age group are susceptible to be victims of ‘Child Pornography’. There is a law which has been framed for the children under the age of 13 [Childrens’ Online Privacy Protection Act], wherein Parental permission is required while a child is being advertised on the electronic media or otherwise.

REFERENCES


10. http://www.cyberlaws.net/itamendments/IT

11. http://www.dailymobile.org/networksecurity