Paper Presentation

On

'IT Policy and Cyber Law in Nepal'

Documents Prepared by

Mr. Rabin Lamichhane
Mr. Saroj Pandey
Mr. Shiba Ratna Tamrakar

(BCA 6th Semester)

Documents Submitted to

Mrs. Parbati Rajbhandari

Wednesday, August 16 2006

Kantipur City College

(Affiliated to Purbanchal University)
Putalisadak, Kathmandu.

Acknowledgment

This research is an experience in itself. We worked hard to have information in IT Policy and Cyber law in the prospective of Nepal and prepare this document to this stage. There are numbers of peoples behind successfully completion of our project, so we would like to appreciate all for their generous support.

We express our gratitude to our faculty Mrs. Parbati Rajbhandari and Mr. Manil Shrestha for helping on every steps.

We are also equally grateful to "KANTIPUR CITY COLLEGE" for providing us this opportunity to have the new experience.

---------- ---------- ----------

Rabin Lamichhane **Saroj Pandey** **Shiba Ratna Tamrakar**

(4021 CA03) (4029 CA03) (4032 CA03)

[Research Group Members]

TABLE OF CONTENT

Chapter 1

Introduction

1.1 Background

The worlds least developed countries including Nepal have availed themselves of the opportunity to rapidly develop education, health, agriculture, tourism, trade and various other sectors using Information Technology. To place the Nepal in the global map of information technology certain objectives, strategies and action plans are need to be followed so to fulfill these requirements the government of Nepal has declared 'Information Technology Policy – 2000'. The main objective of that Policy is to make information technology accessible to the general public and increase employment, to build a knowledge-based society and to establish knowledge-based industries.

With the large development of Information Technology the criminal activities are also increasing so to control those criminal acts and make the digital communication and data secured the Cyber Law came into it's existence. In Nepal also Cyber crime like Software Piracy, Hacking etc. are increasing. Corruption is seen in every field. Big government and some private organizations are using pirated CDs. Even some security organizations responsible for taking action against this crime are seen as violating
the rules. Software CDs can be seen in the footpaths of Kathmandu, which has decreased the value, as well as violated the newly implemented law of the country. People are crowding into these places because the price is low. People want just the CDs. Who cares about the quality and law?

Program CDs of great value are found all over the Kathmandu valley and prices range from Rs. 50-100 (U.S.$0.70 -1.40). Though this is not new to any Nepali citizen, it may attract the attention of some foreigners visiting Nepal. “Foreigners are taking numerous pirated software CDs back to their countries”, said one Footpath CDs seller in
Kathmandu. This problem is not limited to CDs. Even in Cybercafes, children of young ages can be seen using porn sites. The proprietor of the Cafe, not caring about the law, just wants all his computers to be packed. Different hacker software can be found in each individual's computer. Whenever anyone buys a new software CD, it is shared with all his friends and relatives. So, it has become a habit for all Nepali people to share CDs.

To control these activities the 'Electronic Transaction Act' is declared by Ministry of Information Technology and Telecommunication in 2061 B.S [2005 A.D.] which is popularly known as Cyber Law. This is not fully approved as law so it’s renewed in every 6 months. This law gave the new trust to IT Professionals for favorable working situation. This include the provisions to electronic communication, data exchange and other issues and activities of cyberspace.

1.2 Cyber Crimes

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As Cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current status to determine whether they are sufficient to combat the kinds of crimes.

In today's world Cyber crime is a big challenge for security personals. Cyber crime consists of specific crimes dealing with computers and networks (such as hacking, stealing) and the facilitation of traditional crime through the use of computers (child pornography, hate crimes, telemarketing /Internet fraud). In addition to cyber crime, there is also "computer-supported crime" which covers the use of computers by criminals for communication and document or data storage. While these activities might not be illegal in and of themselves, they are often invaluable in the investigation of actual crimes. Computer technology presents many new challenges to social policy regarding issues such as privacy, as it relates to data mining and criminal investigations.

Here are the some mostly happened Cyber crimes in our Cyberspace:-

1.2.1 Hacking

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from most of the Laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information which is critical in nature.

1.2.2 Child Pornography

The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet is very fast becoming a household commodity. Its explosion has made the children a viable victim to the Cyber crime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of pedophiles.

1.2.3 Cyber Stalking

Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the Cyber criminal towards the victim by using Internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker.

1.2.4 Denial of service Attack

This is an act by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with Spam mail depriving him of the services he is entitled to access or provide.

1.2.5 Virus Dissemination

Malicious software that attaches itself to other software. virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious.

1.2.6 Software Piracy

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

1.2.7 IRC Crime

Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other.

1.2.8 Credit Card Fraud

The unauthorized and illegal use of a credit card to purchase property.

1.2.9 Net Extortion

Copying the company's confidential data in order to extort said company for huge amount.

1.2.10 Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

1.3 Cyber law

Cyber law encompasses a wide variety of legal issues related to use of communications technology. It includes use of Internet as well as any other form of Computer or Digital Processing Devices. It includes intellectual property, privacy, freedom of expression, and jurisdiction. Cyber Law addresses the issues of Virtual Property and Virtual Persons. It covers rights of Netizens who are the citizens of Cyber Space and regulation of the Cyber Space for a peaceful and harmonious existence of Netizens. The biggest challenge before Cyber Law is its integration with the legacy system of laws applicable to the physical world. Since Cyber Space has no geographical boundaries, nor the Netizens have physical characteristics of Sex, Age etc, several conflicts surface when the rights of Netizens are viewed in the eyes of Citizens of a physical space. This is well reflected in the conflict between the Trade mark Laws and system of Domain Names. There are several countries which have enacted special laws for regulating Cyber Space Transactions of Citizens within their Physical Jurisdiction and these are recognized as the Cyber Laws of the Physical Jurisdiction.

1.4 General Tips

1.4.1 Take a test before opening e-mail attachment

Is the email from someone that you know?
Have you received email from this sender before?
Were you expecting email with an attachment from this sender?

1.4.2 Make your computer secure

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as “intruders”) from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

1.4.3 Use Strong Password

For each computer and service you use (e-mail, chatting, online purchasing, for example), you should have a strong password.

1.4.4 Protect Your Website

Stay informed and be in touch with security related news.

1.4.5 Protect Your Personal Computer

Use the latest version of a good anti-virus software package which allows updating from the Internet.

1.4.6 Tips for Children

Do not give out identifying information such as name, home address, and school name or telephone number in a chat room.

1.5 Cyber Ethics

We live in an exciting time in history. The widespread availability of computers and Internet connections provides unprecedented opportunities to communicate and learn. Unfortunately, although most people use the Internet as a powerful and beneficial tool for communication and education, some individuals exploit the power of the Internet for criminal or terrorist purposes. We can minimize the harm that such individuals do by learning ourselves, and teaching young people, how to use the Internet safely and responsibly. The term "Cyber Ethics" refers to a code of safe and responsible behavior for the Internet community. Practicing good Cyber Ethics involves understanding the risks of harmful and illegal behavior online and learning how to protect ourselves, and other Internet users, from such behavior. It also involves teaching young people, who may not realize the potential for harm to themselves and others, how to use the Internet safely and responsibly.

Chapter 2

An Ordinance to provide the provisions for Electronic Transaction 2061 B.S. [2005 A.D.]

In the year 2061 the ministry of Information technology and telecommunication have declared an ordinance on Cyber activities, to make immediately the legal provisions for authentication and regularization of the recognition, validity, integrity and reliability of generating, producing, processing storage communication and transmission system of electronic record by making the transaction to be carried out by electronic data exchange or any means of electronic communication and that is popularly known as Cyber Law.

2.1 Provisions in Cyber Law

- ***Provisions relating to electronic record and digital signature.***
    - **Authenticity of Electronic Record.**
        - Any subscriber may, subject to the provisions of this section authenticate to any electronic record by his/her digital signature. Any person may verify the electronic record by using the public key of the subscriber.
    - **Legal Recognition of Electronic Record.**
        - If any information, documents, records or any other matters are maintained in an electronic from by filling the procedures as stipulated in the Ordinance or the Rules made hereunder, such electronic records shall also have legal validity.
    - **Legal Recognition of Digital Signature.**
        - If any information, documents, records or any other matters are certified by the digital signature after fulfilling the procedures as stipulated in the Ordinance such digital signature shall also have legal validity.

- **Electronic Records to be kept safely.**
    - The law in force requires any information, document or records to be kept safely for any specific period of time and if such information, documents or record are kept safely in electronic form and will have legal validity if they fulfill following conditions :
        1. Kept in accessible condition making available for a subsequent reference.
        2. Kept Safely in the format that can be demonstrated subject to presenting again exactly in the same format in which they were originally generated and transmitted or received or stored.
        3. Kept making the details available by which the origin, destination and transmission or date and time of receipt can be identified.

- **Electronic Records May Fulfill the requirement of submission of any Original Documents.**
    - Any record shall have to be submitted or retained in its main or original form or kept safely then such requirement be deemed to have been satisfied by electronic records.

- ***Provisions relating to dispatch receipt of electronic record.***
    - Electronic records to be attributed to Originator.
    - Procedure of Receipt and acknowledgment of Electronic Record.
    - Time and place of Dispatch and Receipt of Electronic Records.

- ***Provisions relating to controller and certifying authority.***
    - Appointment of the controller and other employees.
    - Function, Duties and powers of the Controller.
    - License to be obtained.
    - Application to be submitted for a license.
    - Procedure for granting licenses.
    - Renewal of licenses.
    - Suspension of licenses.
    - Notice of suspension and revocation licenses.
    - Recognition of foreign certifying authority.
    - Performances audit of certifying authority.
    - Controller to have access to the Computers and data.
    - Records to be maintained.

- ***Provisions relating to Digital Signature and Certificates.***
    - Certifying Authority may Issue of the Certificate.
    - Application to obtain Certificate.
    - Suspension of Certificate.
    - Revocation of Certificate.
    - Notice for Suspension and Revocation.

- ***Functions, Duties and Rights of the Subscriber.***
    - To Generate Key Pair (Private and Public Key).
    - To Accept the Certificate.
    - To retain the Private key in a secured manner.
    - Deposit the private key to the Controller.

- ***Electronic Record and government use of Digital Signature.***
    - Government documents may be published in digital form.
    - Accepting the Documents in digital form.
    - Use of Digital Signatures in government offices to verify the electronic data.

- ***Provisions relating to Network Services.***

  This includes the conditions regarding to the Network Service Provider and the Subscriber.
    - Liability of Network Service Provider
    - Network Service Provider not to be Liable.

- ***Offense Relating to Computers.***
    - Pirate, Destroy or Alter Computer Source Code.
    - Unauthorized Access in Computer Materials.
    - Damage to any Computer and Information System.
    - Publication of illegal materials in electronic form.
    - Confidentiality to Divulge.
    - To inform False statement.
    - Submission or Display of False License or Certificates.
    - Non-Submission of prescribed Statement or Documents.
    - Commit Computer Fraud.
    - Abutment to commit computer related Offenses.
    - Punishment to the Accomplice.
    - Punishment in an Offense committed outside Nepal.
    - Confiscation.
    - Offense committed by a corporate body.

- ***<u>Provisions relating to Information System Tribunal.</u>***
    - Constitution of the tribunal.
    - Qualification of the member of the Tribunal.
    - Terms of office, remuneration and conditions of services of the member of tribunal.
    - Circumstances under which office shall be fallen vacant and filling up of vacancy.
    - Staff of the Tribunal.
    - Procedures to be followed by the tribunal.

Chapter 3

Information Technology Policy - 2000

3.1 Introduction

While protecting your organization from outside threats is clearly important, protecting the organization from internal threats is at least as important, if not more so. According to the 1999 **Computer Crime and Security Survey** conducted by the **Computer Security Institute and the FBI**, 55% of the respondents reported unauthorized access to information by persons inside the organization, compared to just 30% who reported intrusions by outsiders. A quarter reported theft of proprietary information and 69% reported theft of laptop computers. Ninety percent (90%) reported virus contamination and a staggering 97% reported systems abuse by insiders (pornography, pirated software, inappropriate email usage, etc.). According to Sex tracker, an organization that tracks the on line pornography trade, seventy percent (70%) of on line pornography viewing occurs during the 9-5 workday.

Although some companies have instituted rudimentary email usage policies, most have neglected to address all aspects of computers in the workplace and information security. Although the best-crafted policies may not stop an employee bent on violating them, good policies will minimize their opportunities and minimize the organization's liability.

Organizations of all sizes often suffer from the same computer and information security problems, many of which are easy to correct. Individuals trying to gain access to your computer systems and data often exploit these security holes. This guide will discuss these and how proper policies and procedures can plug these holes.

Perhaps the most common threat to organizations comes from viruses, worms, and other hostile programming code. While it may be impossible to completely guard against all such threats, following the policies set forth in this manual will minimize the threat potential. The steps include educating your users to the threats, setting out policies that minimize the infection potential, installing anti virus software, regularly updating the anti virus software, and installing all of the security patches for operating systems, web browsers, email clients, and applications.

Many sample policies refer to the "Information Resources Department" or the "Director of Information Resources." If your company uses another designation for these, simply replace the terms with the appropriate ones. If your company is smaller and does not have such a section of individual, consider designating someone to be the Director of Information Resources; this does not have to be a full-time position and can be in addition to the person's existing duties. Having a single focal point for your information resources will streamline handling computer related issues; users will know who to ask for clarifications to policies and who to report violations to.

Likewise, references to "The Company" should be replaced with your organization's name.

The term "user", instead of "employee", was chosen so that the policies would encompass employees as well as contractors or other non-employees that have access to the organization's computers.

All users should be provided a copy of the computer policies and required to sign a statement that they have received them, read them, understand them, and agree to abide by them. This applies to all existing employees, contractors, temporary workers as well as all new personnel. A sample acknowledgment statement is included at the end of the policy guide.

Several policies contain notifications to system users that they have no expectation of privacy. While they may appear redundant, they serve to reinforce the absolute lack of privacy. Courts have generally ruled in the favor of employers where policies made it clear that the employee had no expectation of privacy.

The Courts and federal regulators have generally left employers to regulate personal computer, Internet, and email usage as the employer wishes. You should be aware, however, of the National Labor Relations Board (NLRB). The Depression-era National Labor Relations Act protects workers who are communicating about work terms and conditions; this includes union activity, salary, sick time, and vacation time. While in 1988 the NLRB upheld the firing of an employee that sent an email critical of layoffs, where the email was sent at a busy time of the day and disrupted the companies computer system, in 1998 they ordered a company to rehire an employee that was fired for criticizing a leave policy via email.
The difference in the two cases, other than the political time frame, appears to be that the first worker physically disrupted his employer's business. The second employer did not physically disrupt the business, but angered management by criticizing a new policy. The NLRB General Counsel's Office has issued an opinion memorandum stating that an employer cannot ban employee use of email for messages that are federally protected under labor law.

For purposes of policies, employers may wish to consider the federally protected communications as work related, not personal use. If your organization is unionized, you should consult with a knowledgeable attorney before implementing any policies that might affect union employees.

You should thoroughly read all of the policy areas, even ones that you think may not apply. Because all of the topics are inter-related, the discussion of one may provide you with additional insight into another.

Wherever possible, Login banners should be displayed that reiterate key points of the organization's computer policies. The further reinforcement provided by the login banners should also serve to

strengthen the organization's right to inspect email and other computer files should employee litigation occur. A sample login banner is included in the policy guide.

The days of an employee spending their entire career at a single employer are long past. Workers often leave for a minimal pay increase; in some fields, this is the only way to increase one's salary. With this highly mobile workforce comes a lessened loyalty to employers. It is incumbent upon employers to protect their assets from the plethora of liabilities created by the information age.

3.2 IT Policy in Nepal

World is emerging into a small Cyber world and Nepalese government also took first step toward it in year 2057 B.S. IT Policy was introduced as a means to develop IT sector in Nepal. At the same time government have promise to built IT Park in Banepa, Kabhre which is now only a dream.

The main vision of IT Policy is

"To place Nepal on the global map of information technology within the next five years."

- **Three main objectives are:**
  - To make information technology accessible to the general public and increase employment through this means,
  - To build a knowledge-based society, and
  - To establish knowledge-based industries.

- **Major Strategies suggested by IT Policy 2000 A.D.**
  - The government shall act as a promoter, facilitator and regulator.
  - High priority shall be given to research and development with participation of private sectors.
  - Nepal shall be placed on the global map of information technology
  - E-commerce shall be promoted with legal provisions as well as e-governance should be implemented.
  - Computer education shall be incorporated in academic curriculum starting from the school level.
  - Export of services related to information technology (software and hardware) shall be increased to 10 billion rupees within the next five years.

- **Main Policies**
  - To declare IT sector a priority sector.

- To computerize the system in all government offices and build their web-sites for the flow of information.
- To establish a national information technology Center
- To establish computer education in the curriculum starting from the school levels and broaden its scope.

- **Action Plan**
  - Participation of private sectors in infrastructure development.
  - Infrastructure development.
  - Human Resource Development.
  - Dissemination of Information Technology.
  - Facilities to Information Technology Sectors.

- **Institutional Provisions**
  - Constitute the National Information Technology Development Council under the chairmanship of the Honorable Prime Minister and that council will review and revise the information policies.
  - Carry out different researches and develop information technology manpower with computer trainings and establish relations with foreign educational institutes.
  - The National Information Technology Centre.
  - Information Technology Park Development Committee.

- **Legal Provisions**

  Necessary laws shall be enacted to regulate transaction to be carried out through Information Technology.

3.3 Effect of published IT Policy.

- Many people were trained by the Ministry of Information Technology and communication.
- IT Professionals were encouraged to start better software and hardware development.
- Many students were encouraged to choose computer and communication as their major subject for study.
- Many Multinational industries were became interested to establish IT industries in Nepal.

3.4 Causes of failure of IT Policy

- The most important failure cause of IT Policy 2000 A.D. was the unstable government.
- The lack of high speed telecommunication and Internet facility.

- Lack of specialized and experienced IT professional (Only few exist).
- Lack of proper resources.
- Lack of financier.
- Due to limitation of highly education people in few numbers.
- Lack of knowledge in general public about the importance of computer and telecommunication in their daily life.
- Lack of academic curriculum of computer study from school level.
- Because the objective the IT Policy aimed was very ambitious, people even don't know about IT, but the policy maker aimed to build knowledge-based society, which is even a subject of research for developed countries. May be the policy maker misuse the word knowledge-based with different meaning than it actually has in IT terminology.

Chapter 4

4.1 Conclusion

Laws are established and enforced by the authority, legislation, or custom of a given community, state or nation to maintain orderly coexistence. Basically, Cyber law deals with child pornography, Cyber-stalking, Cyber-scams, online fraud, software piracy and much more. Legal experts are working in this field to help educate and guide the Internet community on crime prevention and the reporting of Cyber crimes. After many years of discussion and effort, government of Nepal has crafted the much awaited Electronic Transaction and Digital Signature Act-Ordinance 2061 but there are much doubts on successful implementation. Because Nepalese think that "laws are made to be broken". This current Cyber Law has failed to address many problems. The law is not stringent enough for the holistic deception of Cyber related crimes. Problems of online media, as well as fines and imprisonment, are not as big as in the U.S. and Japan.

The effective implementation of Cyber law will be a necessity. Nepal will not be able to regulate the information technology industries without taking the international legal context into account. The main thing is that regulations are enforced. First of all, the authorities should be self-concerned before awaking the citizens. There still needs a lot of homework to be done if Nepal expects a boom in the IT sector.

Anyway this law has provided new trust to the Information Technology (IT) sector, and computer and IT professionals are hopeful that it will create a favorable situation for conducting IT business. It contains a strong provision of punishment against Cyber crimes according to the nature of the crime. As per the provisions of law, the government is fully authorized to punish Cyber criminals -- both an individual or
institution.

Since the computing field is a dynamic one, policies and laws related
to this area need to be revised periodically to reflect the changing
trends. At both levels -- the local as well as global.

4.2 Recommendation

We cannot say that Law itself will solve all the problems, but we can also think of different solutions to different problems. First of all the government need to make the people aware of all these laws and policies. We suggest 3 kinds of actions to secure from Cyber crimes:-

1. Company should secure their networked Information.
2. Government should assure that they can implement law fully.
3. Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for Cyber security.

Most great Cyber crime in Nepal is Software Piracy so to control this problem government and private IT Companies should aware the people to use free/open sources softwares so that they can get it free of cost. The government and private IT Companies should try to migrate to free operating environment.

4.3 Bibliography

1. http://www.cybercellmumbai.com/cyber-crimes/
2. http://www.dfait-maeci.gc.ca
3. http://www.rehmantech.com/policy/
4. http://en.wikipedia.org/wiki/cyber_law
5. http://www.nta.gov.np/cyber_law.html
6. http://www.citizenceafre.virtualpune.com/htl/cyber_crimes.shtml
7. http://www.seclists.org/isn/2006/feb/0030.htm
    - Article on “Nepal's Current Situation” by Bishnu KC