Unit-4
Legal Issues in Cyber Crime

- Legal Issues in Information Security
- Cyber Law in Nepal
- Security Policy
- Managing Risk
- Information Security Process
- Information Security Best Practice

Legal issues in Information Security:

- It is true that any business operates in a legal environment.
- Liability, copyright, jurisdiction etc. are some of the legal issues related to information security.

Issues of copyright and trademarks:

- Internet Copyright and trademark violation fall under intellectual property law.
- Intellectual property includes software, music, videos, books, trademarks, copyright and web pages.
- Copyright is ownership of an original work created by the author.
- Trademark represents a symbol or picture that identifies the product or service is intellectual property.

Issue of jurisdiction:

- Jurisdiction is the official power to make legal decisions and judgements.
- The internet is beyond geographic borders, there are no laws or border on the internet.
- Different countries have a different legal system, criminal laws and consumer protection laws which makes e-commerce business difficult to run business over the internet.

Cyber Law in Nepal

Cyberlaw is the area of law which concerns computers and computer-related crimes.
It merges many legal sides including

- Internet law and regulations
- Telecommunication laws
- Software laws
- International laws
- Criminal law
- Intellectual property law etc.

And puts them into the context of computers.
Generically, cyber law is referred to as the Law of the Internet.

- Nepal's Cyberworld is ruled by the Electronic Transaction Act (ETA) 2063 that protects users online against cybercrimes.
- The Act is dived into 12 sections and 80 clauses. This law keeps an eye on issues which are related to computer networks and cybercrime.
- It brings cyber criminals under the justice of law and penalizes them just like other crimes. As per the Act, if anyone is found violating cybercrime, he/she will be punished for a minimum of 6 months to a maximum of 3 years in jail and has to pay minimum 50 thousand to maximum 3 lakhs as a penalty.

Some of the major provisions are:

1. It has the provision relating to electronic records and digital signature.
2. It has the provision relating to dispatch, receive an acknowledgement of electronic records.
3. It has the provision relating to government use of the digital signature.
4. It has a provision relating to the computer network and network services providers.
5. It has the provision relating to computer-related crimes and punishments.

Security Policy

- A security policy is a written document in an organization outlining
    - how to protect the organization from threats, including computer security threats,
    - and how to handle situations when they do occur.
- A security policy must identify all of a company's assets as well as all the potential threats to those assets.
- Thus, an effective IT security policy is a unique document for each organization, cultivated from its people's perspectives on risk tolerance, how they see and value their information, and the resulting availability that they maintain of that information.

Need of Security policies-

1) It increases efficiency.

- The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources.
- The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) It upholds discipline and accountability

- When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law.
- The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can make or break a business deal

- It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information.

- It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4) It helps to educate employees on security literacy

- A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data.
- It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

There are some important cybersecurity policies recommendations describe below-

1. Virus and Spyware Protection policy

- This policy provides the following protection:
    - It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
    - It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.

2. Firewall Policy

- This policy provides the following protection:
    - It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
    - It detects the attacks by cybercriminals.
    - It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. Application and Device Control

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.

5. Exceptions policy

- This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

6. Host Integrity policy

- This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure.
- This policy requires that the client system must have installed antivirus.

Managing Risk

- Risk management is the action of prioritizing cybersecurity measures in regards to possible consequences of vulnerabilities within the process.
- IT professionals depend on technologies and combinations of strategies to protect their organization against cybercrime.
- Cybersecurity risk management is similar to real-world risk management, but takes place in the cyber world.
- The need for cybersecurity risk management grows as the volume of compromised systems, stolen data, and damaged reputation increases with hundreds of cybercrimes happening every day.

The cyber risk management process

Although specific methodologies vary, a risk management program typically follows these steps:

1. **Identify** the risks that might compromise our cyber security. This usually involves identifying cyber security vulnerabilities in our system and the threats that might exploit them.
2. **Analyze** the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.
3. **Evaluate** how each risk fits within your risk appetite (your predetermined level of acceptable risk).
4. **Prioritize** the risks. Decide how to respond to each risk.
5. **Treat** – modify the likelihood and/or impact of the risk, typically by implementing security controls.
    - Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).

- Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
- Transfer – share the risk with another party, usually by outsourcing or taking out insurance.

6. Since cyber risk management is a continuas process**, monitor** risks to make sure they are still acceptable, review controls to make sure they are still fit for purpose, and make changes as required. Remember that risks are continually changing as the cyber threat landscape evolves, and systems and activities change.

Information Security Process

- Information security process is a process that moves through phases building and strengthening itself along the way.
- Although the Information Security process has many strategies and activities, we can group them all into three distinct phases **- prevention, detection, and response**. Each phase requiring strategies and activities that will move the process to the next phase.
- The ultimate goal of the information security process is to protect three unique attributes of information. They are:

Prevention: Preventing an incident requires careful analysis and planning. Information is an asset that requires protection commensurate with its value. Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional. During the prevention phase, security policies, controls and processes should be designed and implemented.

Detection: Detection of a system compromise is extremely critical. With the ever-increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. Intrusion detection systems (IDS) are utilized for this purpose. IDS have the capability of monitoring system activity and notifies responsible persons when activities warrant investigation.

Response: For the detection process to have any value there must be a timely response. The response to an incident should be planned well in advance. Making important decisions or developing policy while under attack is a recipe for disaster. Many organizations spend a tremendous amount of money and time preparing for disasters such as tornados, earthquakes, fires and floods. A Computer Security Incident Response Team (CSIRT) should be established with specific roles and responsibilities identified. These roles should be assigned to competent members of the organization. A team leader/manager should be appointed and assigned the responsibility of declaring an incident, coordinating the activities of the CSIRT, and communicating status reports to upper management.

Information Security Best Practice

1. Install anti-virus software and keep all computer software patched. Update operating systems, applications, and antivirus software regularly.
2. Use a strong password and don't reuse same passwords for different accounts.
3. Log off (Log out) from public computers such as office, hotel or café etc.
4. Back up important information and verify that you can restore it.
5. Keep personal information safe.
6. Be wary of suspicious e-mails and never ever respond to emails asking you to disclose any personal information.
7. Pay attention to browser warnings and shop smart online and don't click everywhere.
8. Download files legally.
9. Secure your laptop, smart phone or other mobile devices
10. Consider biometric security