Cyber Law: Everything You Need to Know

Cyber law is any law that applies to the internet and internet-related technologies and is one of the newest areas of the legal system.

What Is Cyber Law?

Cyber law is any law that applies to the internet and internet-related technologies. Cyber law is one of the newest areas of the legal system. This is because internet technology develops at such a rapid pace. Cyber law provides legal protections to people using the internet. This includes both businesses and everyday citizens. Understanding cyber law is of the utmost importance to anyone who uses the internet. Cyber Law has also been referred to as the "law of the internet."

Cybercrime and Cyber security

Areas that are related to cyber law include cybercrime and cyber security. With the right cyber security, businesses and people can protect themselves from cybercrime. Cyber security looks to address weaknesses in computers and networks. The International Cyber security Standard is known as ISO 27001.

Cyber security policy is focused on providing guidance to anyone that might be vulnerable to cybercrime. This includes businesses, individuals, and even the government. Many countries are looking for ways to promote cyber security and prevent cybercrime. For instance, the Indian government passed the Information Technology Act in 2000. The main goal of this law is to improve transmission of data over the internet while keeping it safe.

Information is another important way to improve cyber security. Businesses, for example, can improve cyber security by implementing the following practices:

- Offering training programs to employees.
- Hiring employees who are certified in cyber security.
- Being aware of new security threats.

Cybercrimes can be committed against governments, property, and people.

Categories of Cyber Crime

Generally, there are three major categories of cybercrimes that you need to know about. These categories include:

- **Crimes Against People.** While these crimes occur online, they affect the lives of actual people. Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online related libel or slander.
- **Crimes Against Property.** Some online crimes happen against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violations.
- **Crimes Against Government.** When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty and an act of war. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

Most of these types of cybercrimes have been addressed by the IT ACT of 2000 and the IPC. Cybercrimes under the IT ACT include:

- Sec. 65, Tampering with Computer Source Documents.
- Sec. 66, Hacking Computer Systems and Data Alteration.
- Sec. 67, Publishing Obscene Information.

- Sec. 70, Unauthorized Access of Protected Systems.
- Sec. 72, Breach of Confidentiality and Privacy.
- Sec. 73, Publishing False Digital Signature Certificates.

Special Laws and Cybercrimes under the IPC include:

- Sending Threating Messages by Email, Indian Penal Code (IPC) Sec. 503.
- Sending Defamatory Messages by Email, Indian Penal Code (IPC) Sec. 499
- Forgery of Electronic Records, Indian Penal Code (IPC) Sec. 463
- Bogus Websites & Cyber Fraud, Indian Penal Code (IPC) Sec. 420
- Email Spoofing, Indian Penal Code (IPC) Sec. 463
- Web-Jacking, Indian Penal Code (IPC) Sec. 383
- Email Abuse, Indian Penal Code (IPC) Sec. 500

There are also cybercrimes under the Special Acts, which include:

- Online Sale of Arms Under Arms Act, 1959
- Online Sale of Drugs Under Narcotic Drugs and Psychotropic Substances Act, 1985

Cyber Law Trends

Cyber law is increasing in importance every single year. This is because cybercrime is increasing. To fight these crimes, there have been recent trends in cyber law. These trends include the following:

- New and more stringent regulations.
- Reinforcing current laws.
- Increased awareness of privacy issues.
- Cloud computing.
- How virtual currency might be vulnerable to crime.
- Usage of data analytics.

Creating awareness of these issues will be a primary focus of governments and cyber law agencies in the very near future. India, for instance, funded cyber trend research projects in both 2013 and 2014. In addition, India held an international conference related to cyber law in 2014. This was meant to promote awareness and international cooperation.

Cyber Law and Intellectual Property

An important part of cyber law is intellectual property. Intellectual property can include areas like inventions, literature, music, and businesses. It now includes digital items that are offered over the internet. IP rights related to cyber law generally fall into the following categories:

- **Copyright.** This is the main form of IP cyber law. Copyrights provide protection to almost any piece of IP you can transmit over the internet. This can include books, music, movies, blogs, and much more.
- **Patents.** Patents are generally used to protect an invention. These are used on the internet for two main reasons. The first is for new software. The second is for new online business methods.
- Trademarks/**Service Marks.** Trademarks and service marks are used the same online as they are in the real world. Trademarks will be used for websites. Service marks are used for websites that provide services.
- **Trade Secrets.** Trade secret laws are used to protect multiple forms of IP. This includes formulas, patterns, and processes. Online businesses can use trade secret protections for many reasons. However, it does not prevent reverse engineering.
- **Domain Disputes.** This is related to trademarks. Specifically, domain disputes are about who owns a web address. For instance, the person who runs a website may not be the person who

owns it. Additionally, because domains are cheap, some people buy multiple domains hoping for a big payday.

- **Contracts.** Most people don't think contracts apply online. This is not the case. For example, when you register for a website, you usually have to agree to terms of service. This is a contract.
- **Privacy.** Online businesses are required to protect their customer's privacy. The specific law can depend on your industry. These laws become more important as more and more information is transmitted over the internet.
- **Employment.** Some employee contract terms are linked to cyber law. This is especially true with non-disclosure and non-compete clauses. These two clauses are now often written to include the internet. It can also include how employees use their company email or other digital resources.
- **Defamation.** Slander and libel law has also needed updating because of the internet. Proving defamation was not altered substantially, but it now includes the internet.
- **Data Retention.** Handling data is a primary concern in the internet age. An area where this has become a big issue is in terms of litigation. In lawsuits, it is now common to request electronic records and physical records. However, there are no current laws that require keeping electronic records forever. This is not true for physical records.
- **Jurisdiction.** Jurisdiction is a key part of court cases. Cybercrime has complicated this issue. If a cybercriminal is located in Minnesota and their victim is located in North Carolina, which state has jurisdiction? Different states have different rules about this issue. Also, it can depend on in what court, federal or state, a case was filed.

Protecting IP can be difficult over the internet. An example of this would be the popularity of pirated movies and music. Each business that relies on the internet needs to develop strategies for protecting their IP. Governments can also take part in this process. In 1999, India did just this by updating their IP laws.

Cyber Security Strategies

Besides understanding cyber law, organizations must build cybersecurity strategies. Cybersecurity strategies must cover the following areas:

- **Ecosystem.** A strong ecosystem helps prevent cybercrime. Your ecosystem includes three areas—automation, interoperability, and authentication. A strong system can prevent cyberattacks like malware, attrition, hacking, insider attacks, and equipment theft.
- **Framework.** An assurance framework is a strategy for complying with security standards. This allows updates to infrastructure. It also allows governments and businesses to work together in what's known as "enabling and endorsing'.
- **Open Standards.** Open standards lead to improved security against cybercrime. They allow business and individuals to easily use proper security. Open standards can also improve economic growth and new technology development.
- **Strengthening Regulation.** This speaks directly to cyber law. Governments can work to improve this legal area. They can also found agencies to handle cyber law and cybercrime. Other parts of this strategy include promoting cybersecurity, proving education and training, working with private and public organizations, and implementing new security technology.
- **IT Mechanisms.** There are many useful IT mechanisms/measures. Promoting these mechanisms is a great way to fight cybercrime. These measures include end-to-end, association-oriented, link-oriented, and data encryption.
- **E-Governance.** E-governance is the ability to provide services over the internet. Unfortunately, e-governance is overlooked in many countries. Developing this technology is an important part of cyber law.

- **Infrastructure.** Protecting infrastructure is one of the most important parts of cybersecurity. This includes the electrical grid and data transmission lines. Outdated infrastructure is vulnerable to cybercrime.

Mitigating Risk

The purpose of cyber law is to reduce risk. This can be done in several ways. Some of the most effective risk reduction strategies of cyber law include the following:

- Cybersecurity Research and Development.
- Threat Intelligence.
- Improved Firewalls.
- The Use of Protocols and Algorithms.
- Authentication.
- Focusing on Cloud and Mobile Security.
- Cyber Forensics.

Another way cyber law can prevent cybercrime is by protecting the supply chain. Interruptions in the supply chain pose big security risks. This is especially true when equipment is allowed to be altered. Protecting the supply chain is key in preventing cybercrime.

Human resource departments can also reduce risk. There are three major ways to do this:

1. Realizing employees may be security risks.
2. Promoting ethical and realistic security mechanisms.
3. Recognizing employees that may be risks.
4. Promoting awareness.

Information sharing is also a key risk-reduction strategy. The best way to do this is with mandatory reporting. When a business is a victim of cybercrime, reporting it right away can reduce further threats. The U.S. promoted this with the Cybersecurity Information Sharing Act of 2014 (CISA).

Lastly, businesses can use a strong security framework. A good framework has three parts:

- **The Core.** These are activities that allow business to identify, protect, detect, respond, and recover from cyber threats.
- **Implementation Tiers.** This describes how advanced a business's security system is. The tiers are Partial, Risk-Informed, Repeatable, and Adaptive. Businesses should strive for the Adaptive tier.
- **Framework Profile.** This is a database where businesses record information about their strategies. This can include concerns and plans for new cybersecurity.

Network Security

Every network needs advanced security. This includes home networks. The most effective way to improve network security is by using the right technology. Network security technology includes the following:

- **Active Devices.** Active devices help a network deal with too much traffic. They also prevent unauthorized traffic. These devices can include either software based or hardware based firewalls, antivirus devices or software, and content filtering devices.
- **Passive Devices.** The most common preventive device is an intrusion detection device. These devices help to recognize unwanted internet traffic.
- **Preventative Devices.** Many devices are focused on preventing network threats. These are called preventative devices. These devices can include network scanners and penetration testers.
- **Unified Threat Management.** These are complete security devices. They can include content filtration, firewall technology, and web caching.

New Cyber Laws

Technology is constantly updating. This means that laws must also be constantly updated. Although U.S. law has remained the same for a long time, five laws were passed in 2014:

- National Cybersecurity Protection Act (NCPA).
- Cybersecurity Enhancement Act of 2014 (CEA).
- Federal Information System Modernization Act of 2014 (FISMA 2014).
- Cybersecurity Workforce Assessment Act (CWWA).
- Border Patrol Agent Pay Reform Act (BPAPRA).

Most of these laws were meant to update existing legislation. FISMA 2014 updated the framework for security controls. NCPA was meant for information sharing between the private sector and the government.

The CEA was one of the most important bills. It may affect private organizations. This is because it promotes developing voluntary cybersecurity standards. This law strengthens the informal mission of the National Institute of Standards and Technology (NIST). The CEA also covers areas once covered by the Federal Financial Institutions Examination Council (FFIEC).

Both the NIST and FFIEC were informal standards. The CEA is a law and more binding. This is particularly useful for resolving disputes resulting from cybercrimes. Businesses need to understand the rules of the CEA.

Cyber Law Business Consideration

The main thing a business needs to understand is their website. A business's website is a large asset. It is also very vulnerable to cybercrime. There are a few issues a business must consider when it comes to their website:

- Who will operate the website?
- Will it be operated on site or off site?
- What security measures will be employed?
- How will email be used, and how will privacy be protected?

It's also important that businesses monitor their IP. A good way to do this is with customer review websites. These sites can both help you identify areas for improvement and can show you if your IP is being used without your permission.

When Customers Use Computers

An important part of complying with cyber law is protecting your customer's personal information. This is true even if your business doesn't have a website.

Many customers make use of online review sites to explain their satisfaction with a company. You can use these sites two ways. First, you can gauge customer satisfaction and identify areas where you can improve. Second, you can use them to see if other businesses are using your name or trademark or if someone is making untrue statements that could harm your business. Either of these issues is eligible for a lawsuit.

Before committing to a business, many customers check the Better Business Bureau (BBB). You should consider joining the BBB. Becoming a BBB member allows customers to trust your company and makes you eligible to use the BBB seal. Potential customers can also find information about your company on the BBB website. If a customer can't find your business on the BBB website, it may cause them to avoid working with your company.

It's also a good idea to make your business's privacy and security policies available to your customers. By allowing them to read these policies, you are proving your dedication to protecting their personal and financial information when they use your website.

ber Law Terms and Laws

There are three main terms that people need to know related to cyber law.:

1. **Information Technology Law.** These laws refer to digital information. It describes how this information is gathered, stored, and transmitted.
2. **Cyber Law/Internet Law.** These laws cover usage of the internet. This is a newer legal area. Many laws can be undefined and vague.
3. **Computer Law.** This covers a large legal area. It includes both the internet and laws related to computer IP.

There have been many countries that have tried to fight cybercrime with cyber laws:

- **Computer Misuse Act 1990 (Great Britain).** This law is mostly focused on data and computer systems. It includes three sections. Section 1 focuses on the unauthorized use of a computer (hacking). Section 2 covers situations where a Section 1 violation has occurred and further offenses are likely. Section 3 is for when a computer is altered illegally. This is usually due to a virus or denial of service act.
- **IT Act of 2000 (India).** This act is focused on information technology. This law both outlines offenses like hacking and trojan attacks, as well as possible solutions. One section outlines the use of digital signatures to improve cybersecurity. Some offenses can compound. This increases their potential punishment.
- **The Middle East and Asia.** Countries across these regions use combinations of cyber laws. In certain countries, these laws are used to prevent citizens from accessing certain information.

Other laws related to cyber law that have been passed by countries around the world include electronic signature laws, information technology guidelines, and information technology laws.

Cyber law has also been used to create privacy. This is particularly true in the United States. U.S. laws that have been used to establish internet privacy include the following:

- Warren and Brandeis.
- Reasonable Expectation of Privacy Test.
- Privacy Act of 1974.
- Foreign Intelligence Surveillance Act of 1978.
- Electronic Communication Privacy Act.
- Driver's Privacy Protection Act.
- Gramm-Leach-Bliley Act.
- Homeland Security Act.
- Intelligence Reform and Terrorism Prevention Act.

Writing and Enforcing Online Laws

The increased use of the internet has changed how older laws need to be enforced. A good example of this is copyright law and the ability for individuals to illegally download music, movies, books, and other forms of intellectual property.

The obstacle in enforcing these laws is that it is hard to trace illegal online activities to their source. Online criminals are often anonymous, and even if a crime can be traced, it is usually only linked to a computer and not a real-life person.

Another difficult is knowing what real world laws apply online. An example of this is internet transactions that take place in multiple countries. For instance, if someone in the USA sells an item to someone in the UK using a server that is located in Germany, the transaction may be regulated by the laws of all three countries.

Internet criminals have tried to take advantage of lax online law enforcement. For instance, over an eight-year period between 2000 and 2008, a company called HavenCo operated servers that were located on a