**Experiment 1**

**Aim** - Study of Different laws and standards of Cyber Security

**Theory**-

A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, 1, or other assets through unauthorized access to a network, computer system or digital device. [Threat actors](https://www.ibm.com/topics/threat-actor) start cyberattacks for all sorts of reasons, from petty theft to acts of war. They use various tactics, like [malware attacks](https://www.ibm.com/topics/malware), [social engineering](https://www.ibm.com/topics/social-engineering) scams, and password theft, to gain unauthorized access to their target systems.

Cyberattacks can disrupt, damage and even destroy businesses. The average cost of a data breach is [USD 4.35 million](https://www.ibm.com/reports/data-breach). This price tag includes the costs of discovering and responding to the violation, downtime and lost revenue, and the long-term reputational damage to a business and its brand.

***Cyber Security attacks :***

Cybercriminals use many sophisticated tools and techniques to start cyberattacks against enterprise IT systems, personal computers, and other targets. Some of the most common types of cyberattacks include:

### 

**Malware** is malicious software that can render infected systems inoperable. Malware can destroy data, steal information, or even wipe files critical to the operating system’s ability to run. Malware comes in many forms, including:

**Trojan horses** disguise themselves as useful programs or hide within legitimate software to trick users into installing them. A remote access Trojan (RAT) creates a secret back door on the victim’s device, while a dropper Trojan installs additional malware once it has a foothold.

**Ransomware** is sophisticated malware that uses strong encryption to hold data or systems hostage. Cybercriminals then demand payment in exchange for releasing the system and restoring functionality. According to IBM’s *X-Force Threat Intelligence Index*, ransomware is the second most common type of cyberattack, accounting for 17% of attacks.

**Scareware** uses fake messages to frighten victims into downloading malware or passing sensitive information to a fraudster.

**Spyware** is a type of malware that secretly gathers sensitive information, like usernames, passwords, and credit card numbers. It then sends this information back to the hacker.

**Rootkits** are malware packages that allow hackers to gain administrator-level access to a computer’s operating system or other assets.

**Worms** are self-replicating malicious code that can automatically spread between apps and devices.

**Social engineering** attacks manipulate people into doing things that they shouldn’t do, like sharing information they shouldn’t share, downloading software they shouldn’t download, or sending money to criminals.

**Phishing** is one of the most pervasive social engineering attacks. According to the *Cost of a Data Breach* report, it is the second most common cause of breaches. The most basic phishing scams use fake emails or text messages to steal users’ credentials, exfiltrate sensitive data, or spread malware. Phishing messages are often designed to look as though they’re coming from a legitimate source. They usually direct the victim to click a hyperlink that takes them to a malicious website or open an email attachment that turns out to be malware.

Cybercriminals have also developed more sophisticated methods of phishing. Spear phishing is a highly targeted attack that aims to manipulate a specific individual, often by using details from the victim’s public social media profiles to make the ruse more convincing. Whale phishing is a type of spear phishing that specifically targets high-level corporate officers. In a business email compromise (BEC) scam, cybercriminals pose as executives, vendors, or other business associates to trick victims into wiring money or sharing sensitive data.

### 

**Denial-of-service (DoS)** and distributed denial-of-service (DDoS) attacksflood a system's resources with fraudulent traffic. This traffic overwhelms the system, preventing responses to legitimate requests and reducing the system's ability to perform. A denial-of-service attack may be an end in itself or a setup for another attack.

The difference between DoS attacks and DDoS attacks is simply that DoS attacks use a single source to generate fraudulent traffic, while DDoS attacks use multiple sources. DDoS attacks are often carried out with a botnet, a network of internet-connected, malware-infected devices under a hacker's control. Botnets can include laptops, smartphones, and Internet of Things (IoT) devices. Victims often don't know when a botnet has hijacked their devices.

### **Man-in-the-middle attacks**

In a man-in-the-middle (MiTM) attack, also called an "eavesdropping attack," a hacker secretly intercepts communications between two people or between a user and a server. MitM attacks are commonly carried out via unsecured public wifi networks, where it's relatively easy for threat actors to spy on traffic. Hackers may read a user's emails or even secretly alter the emails before they reach the recipient. In a session hijacking attack, the hacker interrupts the connection between a user and a server hosting important assets, like a confidential company database. The hacker swaps their IP address with the user's, making the server think they're a legitimate user logged into a legitimate session. This gives the hacker free rein to steal data or otherwise wreak havoc.

**Supply chain attacks** are cyberattacks in which hackers breach a company by targeting its software vendors, material suppliers, and other service providers. Because vendors are often connected to their customers' networks in some way, hackers can use the vendor's network as an attack vector to access multiple targets at once.For example, in 2020, Russian state actors hacked the software vendor SolarWinds and distributed malware to its customers under the guise of a software update (link resides outside ibm.com). The malware allowed Russian spies to access the sensitive data of various US government agencies using SolarWinds' services, including the Treasury, Justice, and State Departments.

***Cyber law***: Cyber Law, also known as internet law or digital law, signifies the legal regulations and frameworks governing digital activities. It covers a large range of issues, including online communication, e-commerce, digital privacy, and the prevention and prosecution of cybercrimes. As the internet has become a fundamental part of our daily lives, cyber law has become crucial in ensuring digital space's orderly and secure functioning.

## ***Significance of Cyber Law:*** The significance of cyber law lies in its capacity to navigate and regulate the intricate challenges that arise from the pervasive use of technology. Cyberlaw provides a framework for protecting individuals and organizations from cyber threats, ensuring the privacy and security of digital transactions, and establishing guidelines for ethical and legal conduct in cyberspace. As the digital world evolves, the importance of cyber law becomes more pronounced, serving as a cornerstone for the responsible and lawful utilization of digital resources.

***Security Standards***

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

## **1. ISO**

ISO stands for International Organization for Standardization. International Standards make things work. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard was officially established On 23 February 1947. It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

### **ISO 27000 Series**

It is the family of information security standards which is developed by the International Organization for Standardization and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organization face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

The ISO 27000 series can be categorized into many types. They are-

**ISO 27001**- This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.

**ISO 27000**- This standard provides an explanation of terminologies used in ISO 27001.

**ISO 27002**- This standard provides guidelines for organizational information security standards and information security management practices. It includes the selection, implementation, operating and management of controls taking into consideration the organization's information security risk environment(s).

**ISO 27005**- This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach. To completely understand the ISO/IEC 27005, the knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is required. This standard is capable for all kind of organizations such as non-government organization, government agencies, and commercial enterprises.

**ISO 27032**- It is the international Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for protecting the information beyond the borders of an organization such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

## **2. IT Act**

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of the United Nations. This act is also used to check misuse of cyber networks and computers in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitates electronic governance by means of reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offenses, and the remaining section 80 to 94 deal with miscellaneous of the act.

## **3. Copyright Act**

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

The copyright act covers the following-

* Rights of copyright owners
* Works eligible for protection
* Duration of copyright
* Who can claim copyright

The copyright act does not covers the following-

* Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
* Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)
* Familiar symbols or designs
* Titles, names, short phrases, and slogans
* Mere variations of typographic ornamentation, lettering, or coloring

**4. Patent Law**

Patent law is a law that deals with new inventions. Traditional patent law protects tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent laws have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

## **5. IPR**

Intellectual property rights is a right that allow creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights. It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

**Conclusion :** Thus we have studied laws and standards of cybersecurity.