International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Security Challenges: Safeguarding Data in the Digital Era

Ms. Rupinder Kaur

Assistant Professor, Dept. of Commerce, Multani Mal Modi College, Patiala, India

ABSTRACT:
The Internet is one of the fastest-growing areas of technical infrastructure development. In today's business environment, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online. Today more than 80 percentof total commercial transactions are done online, so this field required a high qualityof security for transparent and best transactions. The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures. Cyber Security plays an important role in the development of information technology as well as Internet services. Our attention is usually drawnon "Cyber Security" when we hear about "Cyber Crimes". Our first thought on "National Cyber Security" therefore starts on how good is our infrastructure for handling "Cyber Crimes". This paper focus on cyber laws and security emerging trends, issues and challenges while adopting new technologies such as mobile computing, e-commerce, and social networking.

Index Term: Cyber Security, Cybercrimes, Cyber Intelligence, Mobile Internet and Social Networking.

INTRODUCTON:

It can be rightfully said that today almost everybody lies on the Internet. With an increasing amount of people being connected to the Internet, various security threats have emerged which cause massive harm to its users. So now, everybody is on the risk of cyber-attack. As almost all the transactions are done online, there are more chances of cyber-crimes. Therefore, cyber security is required to ensure high quality of security for transparency of all online transactions.

CYBER CRIME: - Cyber-crime is one of the main threats to the digital economy. It encompasses any criminal or unethical activity done by a person with the help of computer or any electronic device-using internet. It is the basic reason for forming cyber laws. These offences are committed against an individual or group of individuals to defraud them, while most of the cybercrimes are carried out in order to generate profits. It includes monetary and non- monetary offences in which the criminals use the Internet to steal personal information from other users. The Council of Europe Convention on Cybercrime defines cybercrime as a wide range ofmalicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements. The rise in widespread use of technology brought with it a rise in cybercrimes.

CYBER SECURITY: - Cyber security is the practice of protecting systems, networks,and programs from digital attacks. It is a defensive solution to protect any internet- connected system from cyber threats and

attacks. It is a complex and challenging problem. Cyber-attacks are fast becoming one of the biggest threats to national security. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting from users; or interrupting normal business processes.

RELEVANCE OF CYBER LAW AND SECURITY:

As information and communication technologies pervade every aspect of our lives-shopping, banking, education and commerce, there are more chances of cybercrimes. So cyber security is important to protect our sensitive data and information from these cyber threats.

Cyber law and security are critically relevant in today's digital age due to several key reasons:

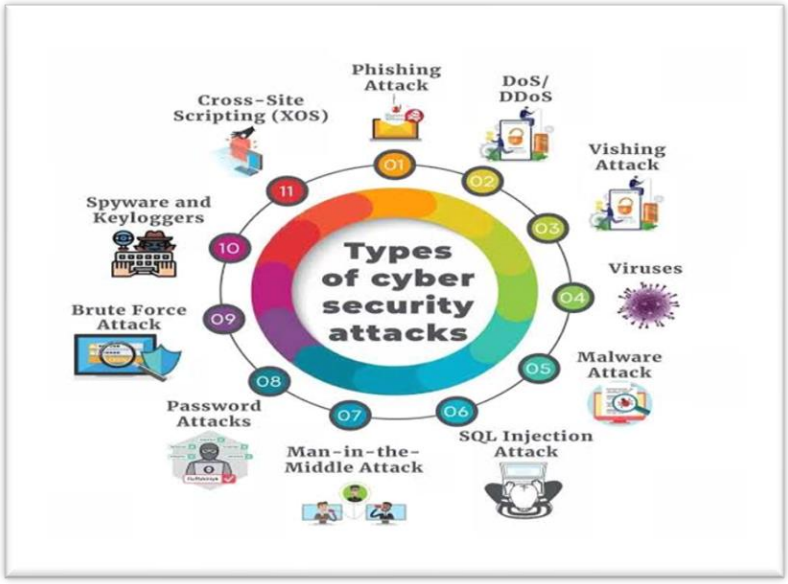
1. **Protection of Personal Data**: With the increasing digitization of personal information, cyber laws ensure that individuals' data is protected from unauthorized access, breaches, and misuse.
2. **Prevention of Cybercrimes**: Cyber laws define offenses such as hacking, identity theft, cyberbullying, and phishing, providing legal frameworks to prosecute offenders and deter such activities.
3. **Regulation of Online Activities**: Laws govern e-commerce, digital contracts, intellectual property rights, and online transactions, ensuring fairness and security in electronic interactions.
4. **National Security**: Cybersecurity measures protect critical infrastructure, government systems, and sensitive information from cyber threats, including espionage and cyberterrorism.
5. **International Cooperation**: With cybercrimes transcending borders, international cyber laws and agreements facilitate cooperation between nations to combat cyber threats effectively.
6. **Business Compliance**: Organizations must adhere to cyber regulations to protect customer data, avoid legal liabilities, and maintain trust and reputation.
7. **Emerging Technologies**: Laws adapt to regulate emerging technologies like AI, IoT, and block chain, addressing privacy concerns and ethical implications.
8. **Education and Awareness**: Cyber laws promote awareness and educate users about safe online practices, cybersecurity measures, and legal implications of cyber activities.

THREATS TO CYBER SECURITY:

- **VIRUSES:** A Virus is a program that is loaded onto your computer without your knowledge and runs against your wishes. Virus dissemination isa process of a malicious software that attaches to other software that destroysthe system of the victim. They disrupt the computer operation and affect the data store by modifying or deleting it. Various types of Viruses are variant virus; overwrite virus; resident virus; polymorphic virus, etc.
- **HACKING:** Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. It means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing personal data, etc.
  Example of hacking: using passwords cracking algorithms to gain access to asystem.
- **MALWARE:** Malware is any software that infects and damages a computer system without the owner's knowledge. It includes viruses and worms, Trojanhorses, Rootkits, Backdoors, Spyware, Botnets, etc.
- **TROJAN HORSES:** Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system. A program allows the attack to control the user's computer

from a remote location. The program is usually disguised as something that is useful to the user.

- **DENIAL-OF-SERVICE (DOS) AND DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS**: DoS attacks flood a network or system with traffic, making it unavailable to users. DDoS attacks amplify this by coordinating multiple systems to simultaneously flood the target.
- **SQL INJECTION**: Attackers exploit vulnerabilities in web applications by injecting SQL commands into input fields to manipulate databases, steal data, or gain unauthorized access.
- **MAN-IN-THE-MIDDLE(MITM):** Attackers intercept and potentially alter communications between two parties without their knowledge. This can allow attackers to steal data or inject malicious content.
- **PASSWORD CRACKING:** Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites. A process of attempting to gain unauthorized access to restricted systems using common passwords or algorithms that guess passwords.
- **PHISHING:** Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information.
  Example: While checking E-Mail one day a user finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately. It is difficult to conclude that it is a fake email.
- **RANSOMWARE:** Ransomware is a type of malicious software, which is designed to extort money by blocking access to files or the computer system until the ransom is paid. It enables cyber extortion for financial gain.
- **KEYLOGGERS:** Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions arebeing monitored. It is a quicker and easier way of capturing the passwords.



ISSUES AND CHALLENGES REGARDING CYBER SECURITY IN PRESENT SCENARIO:

In the present scenario, several key issues and challenges regarding cybersecurity are prominent**:**

1. **Sophistication of Threats**: Cyber threats are becoming increasingly sophisticated, with attackers using advanced techniques such as AI and machine learning to automate attacks and evade traditional security measures.
2. **Rapidly Evolving Technology**: The pace of technological advancement introduces new vulnerabilities faster than they can be addressed, leaving systems susceptible to emerging threats.
3. **Complexity of IT Infrastructures**: Modern IT environments are complex and interconnected, including cloud services, IoT devices, and mobile platforms, which expand the attack surface and make securing them challenging.
4. **Shortage of Skilled Cybersecurity Professionals**: There is a global shortage of cybersecurity experts capable of understanding and mitigating complex threats, leaving organizations vulnerable to attacks.
5. **Insider Threats**: Malicious or negligent actions by insiders, including employees, contractors, or business partners, pose significant risks to organizational cybersecurity.
6. **Regulatory Compliance**: Compliance with data protection regulations (e.g., GDPR, CCPA) adds complexity and costs to cybersecurity efforts, requiring organizations to implement specific measures to protect personal data.
7. **Cybersecurity Awareness and Training**: Lack of awareness and inadequate training among employees and users contribute to human errors and increase the likelihood of successful cyber attacks, such as falling victim to phishing scams.
8. **Supply Chain Vulnerabilities**: Dependency on third-party vendors and suppliers introduces risks, as attackers may exploit weaker links in the supply chain to gain access to sensitive information or disrupt operations.
9. **Persistent Threats (APTs)**: Advanced Persistent Threat actors, including nation-state actors, engage in prolonged and stealthy attacks aimed at espionage, intellectual property theft, or sabotage.
10. **Budget Constraints**: Organizations may face budget limitations that prevent them from investing adequately in cybersecurity tools, technologies, and personnel.

Addressing these challenges requires a holistic approach involving technological solutions, robust policies and regulations, continuous education and training, collaboration between public and private sectors, and proactive risk management strategies. Cybersecurity is not merely a technical issue but a critical aspect of organizational resilience and trust in the digital age.

FUTURE OF CYBER SECURITY:

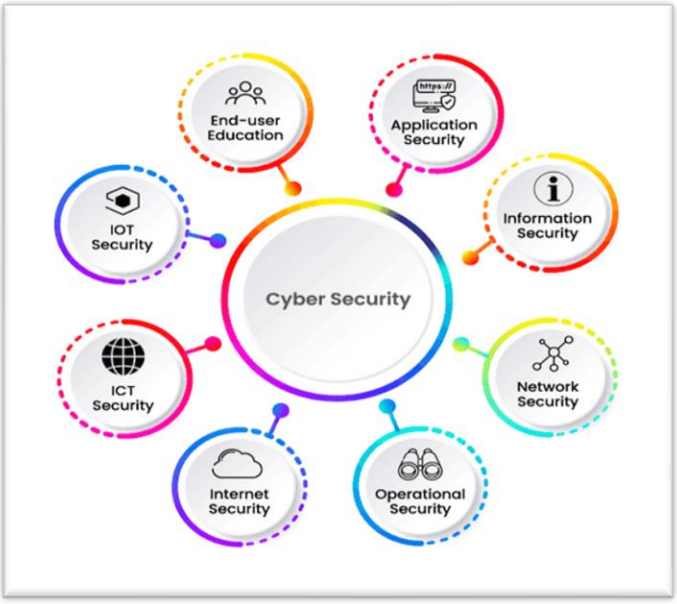
The emerging challenges will drive needs in cyber security. Employers will expect workers to know and apply industry best practices and perspectives. The roles are expanding for incoming cyber security workforce. Resources are emerging to assist academic staff and graduates to understand the needed skill and opportunities**.**

STEPS TO CYBER SECURITY: - Various steps to overcome these cyber-attacks: -

- ***NETWORK SECURITY:*** Protect your networks against external and internal attack. Manage the network primer. Filter out unauthorized access and malicious contents. Monitor and test security

controls.

- ***MALWARE PROTECTION****:* Produce relevant policy and establish anti-malware defenses that are applicable and relevant to all business areas.
- ***MONITORING:*** Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT system and networks. Analyze logs for unusual activity that could indicate an attack.
- ***INCIDENT MANAGEMENT:*** Establish an incident response and disaster recover capability. Produce and test incident managementplans. Provide training to the incident management team. Report criminal incidents to law enforcements.
- ***USER EDUCATION AND AWARENESS:*** Produce user policies covering acceptable and secure use of the organization's systems.Establish a staff-training programme. Maintain user awareness of cyberrisks.
- ***SECURE CONFIGURATION:*** Apply security patches and ensure that the secure configuration of all ICT systems is maintained.
- ***ANTI-VIRUS SOFTWARE:*** Anti-virus software is a computer programthat detects, prevents, and takes actions to remove malicious software programs, such as viruses and worms.
- ***MANAGING USER PRIVILEGES:*** Organizations must create access controls to ensure that employees can access information that is relevant to their job. This prevents sensitive information being exposedshould someone gain unauthorized access to employees' accounts.
- ***REMOVABLE MEDIA CONTROLS:*** Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. USB's and other removable devicesare the source of many security issues. Not only they are often used to inject insider malware but also they are involved in many insider incidents.
- ***USE STRONG PASSWORDS:*** Do not repeat your passwords on different sites, and change your passwords regularly. Make them complex. Passwords must contain a combination of letters, numbers and symbols. A password management application helps to keep our passwords locked down.
- ***ENCRYPT DATA:*** Encryption of data gives the company an upper hand when our data falls into wrong hands. That is because it becomes uselesseven if a hacker sniffs it out, as it is not easy to break the encryption of the data.



SKILLS THAT CYBER SECURITY PROFESSIONALS NEED:

1. **INTRUSION DETECTION:-** A recent survey by Intel Security has found that the cyber security talent deficit is the worst in the IT industry. And intrusion detection is one of the skills in critically short supply. This skill involves discovering threats from outside of a system or organization and detecting threats from within a system or organization; network- based detection attempts to detect unauthorized behavior based on network traffic; while host-based detection looks for illicit activity on a specific device.
2. **SECURE SOFTWARE DEVELOPMENT: -** This is key to any organization's security strategy. Most data breaches are only successful because of frailties in software code. In-house software development is afirst line of defense and if it's sloppy, the hackers will find the holes. As a business owner, you may consider a good quality software developer a bit of ahefty investment. But secure software can help save your business money. Secure code development might cost a little more with the salaries and the testing involved,it's still likely to be far less than an actual breach.
3. **CYBER SECURITY AND RISK MITIGATION: -** This involves identifying and tracking risks, working out future potential risks and planning ahead to avoid risks. Businesses need to identify their most valuable assetsand the risks to these assets. Knowing how the information is stored, who has access and how the data is protected is extremely valuable knowledge in the face of cyber risk. And a risk mitigation specialist will be able to identify all of this and work outways to respond to threats and breaches. Again, in the event of a breach, this'll savea business huge amounts of money.
4. **CLOUD SECURITY: -** As cloud infrastructure develops so it becomes a more lucrative target for cyber criminals. Demand for skills in this field is high as large businesses seek to protect their data. There are several threats to cloud infrastructure. Some of the biggest threats include data breaches, exploiting system vulnerabilities, hijacked accounts, and malicious insiders. This is certainly a skill that'll give the IT graduate enormous employability.

CONCLUSION:

The explosion of the Internet and computer networks allows individuals, businesses,and governments to find and store valuable information, communicate to oneanother, and enjoy the unique methods of making their lives easier. However, this also makes it possible for anyone to perform illegal actions and misuse the powerfultechnology through a variety of means. As the Internet continuous to develop, the potential for computer related crimes would grow. Securing the cyber space presentsmajor challenges. Though not all people are victims to cybercrimes, they are still atrisk. Cyber security is one of the most important aspects of the fast- paced growingdigital world. It is not only essential to business organizations and governmental institutions, but for everyone who is using digital devices like mobile phones, tablets,etc. Every little thing that is connected to the Internet, used for communication and other purposes, can be affected by a breach of security. The changing nature of technology and the sensitivity of information raise the standards needed to protectthe privacy and security of individuals.

REFERENCES:

Books: -

1. Cyber Intelligence by Anju Gautam
2. Cyber Security by Nina Godbole; Sumit Belapure
3. Cyber Surveillance and Security by Yogesh Barua

E- sources: -

1. National Digital Library of India
2. https://www.clickatell.com/articles/information-security/future-cyber- security/
3. https://www.forbes.com
4. https://edition.cnn.com
5. https://www.cisco.com
6. https://www.cybercrimechambers.com
7. https://www.eccouncil.org
8. https://www.deccanchronicle.com
9. https://www.fireeye.com
10. https://www.guru99.com
11. https://www.indiatoday.in
12. https://www.outpost24.com
13. https://www.searchsecurity.techtarget.com
14. https://www.slideshare.net
15. https://www.telstra.com