Research Paper
Impact Factor: 6.304
Peer Reviewed & Indexed Journal
www.iibarr.com

IJBARR
E- ISSN -2347-856X
ISSN -2348-0653

HISTORICAL REVIEW OF CYBER SECURITY IN INDIA

Dr. J. Jeyakumari Gnanadeepam* **Ms. H. Bella Josepha****
**Assistant Professor of History, Sri Meenakshi Government Arts College for Women (A), Madurai.*
***Research Scholar of Commerce, St. Joseph's College (A), Tiruchirappalli.*

Abstract
Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. This article explains the origin of cyber security and its dynamic growth in today's world. History of cybersecurity is marked by the constant cat-and-mouse game between attackers and defenders. The Ministry of Home Affairs oversees the operation of a cyber and information security section that deals with issues related to cyber security, cybercrime, the National Information Security Policy & Guidelines (NISPG) and its implementation, NATGRID, etc. Government Initiatives Related to Cyber Security are highlighted to have knowledge which are prevailing in our country.

Introduction

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against Networked Systems and applications, whether those threats originate from inside or outside of an organization

Origin of cybersecurity

Cybersecurity has a rich history that has evolved alongside the development of computer technology. Here is a brief explanation of the key milestones in cybersecurity history:

1. Early Years: In the 1960s and 1970s, when computers were large and mostly confined to research institutions and government organizations, security concerns were limited. However, as computer networks began to emerge, the need for safeguards became evident.
2. Birth of Hacking: In the 1980s, hacking emerged as a prominent issue. High-profile incidents like the Morris Worm in 1988, which infected thousands of computers, brought attention to the vulnerability of interconnected systems.
3. Encryption Advances: The 1990s witnessed significant advancements in encryption technologies, such as the introduction of the Data Encryption Standard (DES) and later the more secure Advanced Encryption Standard (AES). These encryption algorithms played a crucial role in securing data transmission.
4. Rise of Malware: The 2000s saw a surge in malware attacks, including viruses, worms, and Trojans. Notable examples include the ILOVEYOU worm in 2000 and the Blaster worm in 2003. This period highlighted the need for stronger antivirus solutions and better security practices.
5. Shift to Cybercrime: As the internet became more widely used, cybercriminals increasingly targeted financial institutions, businesses, and individuals for financial gain. Online banking fraud, identity theft, and phishing attacks became prevalent, leading to the development of more sophisticated cybersecurity measures.
6. Advanced Persistent Threats (APTs): APTs emerged in the late 2000s and early 2010s as highly targeted and persistent attacks primarily associated with nation-state actors. Notable APTs include Stuxnet, Duqu, and Flame. These attacks highlighted the need for enhanced security measures and increased international collaboration.

7. Cloud and Mobile Security: The proliferation of cloud computing and mobile devices presented new security challenges. Organizations had to adapt their cybersecurity strategies to protect data stored in the cloud and secure mobile devices accessing sensitive information.
8. Internet of Things (IoT) Security: The rapid growth of IoT devices in homes, industries, and critical infrastructure raised concerns about security vulnerabilities. The Mirai botnet attack in 2016 demonstrated the potential for large-scale IoT-based attacks and the need for robust security measures.
9. Modern Threat Landscape: Today, cybersecurity faces an evolving threat landscape, including ransomware attacks, social engineering, nation-state-sponsored attacks, and supply chain vulnerabilities. There is a growing emphasis on proactive defines, threat intelligence sharing, and the adoption of advanced technologies like artificial intelligence and machine learning for cybersecurity.

Overall, the history of cybersecurity is marked by the constant cat-and-mouse game between attackers and defenders. As technology advances, so do the tactics and tools employed by cybercriminals, requiring ongoing innovation and vigilance to protect against emerging threats.

Cybersecurity warfare

Cyberwarfare is the term used to describe a cyberattack or series of cyberattacks that target a nation. It can disrupt crucial operations and demolish government and civilian infrastructure, harming the state and perhaps even leading to casualties. The bulk of the time, nation-states wage cyberwar by attacking other countries, however on occasion, terrorist organisations or non-state actors launch attacks to support the goals of an enemy state. The term "act of war" in the context of a cyber strike has not been defined, despite the fact that there have been numerous recorded cases of cyber warfare in recent years.

Cyber Attack in India

Delhi AIIMS's servers were recently vulnerable to a ransomware cyber-attack. A ransomware attack on the medical institute's servers has put the personal information of millions of patients at danger. A significant hack against Air India in February 2022 resulted in the compromise of over 4.5 million customer records. Information on a passport, a ticket, and certain credit cards was stolen. Approximately 82% of Indian businesses experienced ransomware attacks in 2020. Juspay, a well-known payment corporation with headquarters in India, experienced a data breach in 2021 that affected 35 million consumers. Juspay handles payments for major firms like Amazon and other online marketplaces, making this breach particularly relevant. The top five Indian cities—Kolkata, Delhi, Bhubaneswar, Pune, and Mumbai—were affected in May 2017.

India's Cybersecurity

With over 900 internet users expected in India by 2025, the concurrent rise in cyber dangers has become increasingly concerning. Cybercrimes are evolving along with digital technologies and getting more complex. India must therefore carefully evaluate the weaknesses in its cyberspace and implement a more comprehensive Cyber-Security Policy to solve them.The Ministry of Home Affairs oversees the operation of a cyber and information security section that deals with issues related to cyber security, cybercrime, the National Information Security Policy & Guidelines (NISPG) and its implementation, NATGRID, etc.

It has the following wings they are Coordination wing, Cyber-crime wing, Information security, Monitoring unit, Cyber-crime coordination centre.

IJBARR
E- ISSN -2347-856X
ISSN -2348-0653

Challenges to India's Cybersecurity

1.Devices used for internet access are not all the same

Due to the broad range of income levels in India, not everyone can afford expensive phones. In the US, Apple has a market share of over 44%. Despite the higher security measures, less than 1% of mobile users in India use iPhones. The rising security gap between premium mobile devices like the iPhone and less expensive ones makes it more challenging for regulators to determine the legal and technical standards for data protection.

2. Lack of National level architecture of cybersecurity

Collaboration between firefighting organizations in the military and the commercial sector that owns critical infrastructure is essential for effectively analyzing and countering various dangers. However, there is currently a lack of a national security architecture that facilitates this unified effort. Recognizing the need for such infrastructure, the Prime Minister's Office has taken steps to address the issue. Despite these efforts, India still lacks the necessary framework and support systems to fully establish the required collaboration and coordination.

3.Lack of separation

Cyberspace has no borders, unlike nations or governments, making it feasible for attacks against the armed forces, the digital assets of ONGC, financial operations, etc. to originate from anyone. This could result in breaches in national security that cost money, assets, or even life. A technically sophisticated multi-agency organisation that can base its decisions on policy inputs and a forceful response plan to possible threats to the country's most priceless resources is required.

4.Lack of awareness

Since there is no national regulatory policy in place for cybersecurity, both businesses and individuals lack awareness. Only in the presence of a regulated and overseen legislative framework can domestic internet users defend themselves and receive protection from cyberattacks.

Government Initiatives Related to Cyber Security

- Indian Cyber Crime Coordination Centre (I4C)
- Information Security Education and Awareness project
- Cyber Surakshit Bharat
- Cyber Swachhta Kendra
- National Cyber Security Coordination Centre (NCCC)
- International cooperation

Indian Cyber Crime Coordination Centre (I4C)

Indian Cyber Crime Coordination Centre (I4C) is an initiative launched by the Government of India to strengthen the country's cybersecurity infrastructure and combat cybercrime. It operates under the Ministry of Home Affairs and aims to enhance coordination among various law enforcement agencies, intelligence agencies, and other stakeholders involved in addressing cyber threats.

Information Security Education and Awareness project: Empowering Users for a Secure Digital Environment

The Information Security Education and Awareness Project is a comprehensive initiative aimed at educating and raising awareness among individuals, organizations, and communities about the

importance of information security. This project recognizes that in an increasingly interconnected world, every user plays a critical role in safeguarding sensitive information and protecting against cyber threats. By providing knowledge, resources, and training, this project seeks to empower users to make informed decisions and adopt secure practices, ultimately contributing to a safer digital environment.

Cyber Surakshit Bharat

Cyber Surakshit Bharat (Cyber Secure India) is an initiative launched by the Government of India with the objective of creating a secure and resilient cyberspace in the country. It is a collaborative effort involving various stakeholders, including government agencies, industry partners, academia, and citizens. The initiative aims to raise awareness about cybersecurity, promote the adoption of best practices, and enhance the overall cybersecurity posture of individuals, organizations, and critical infrastructure.

Cyber Swachhta Kendra

In today's interconnected world, where technology plays a pivotal role in our lives, the need for robust cyber security measures cannot be overstated. Cyber threats, such as hacking, data breaches, and malware attacks, pose significant risks to individuals, businesses, and governments alike. Recognizing the importance of a secure digital ecosystem, the Indian government has taken proactive steps to establish the Cyber Security Swachhta Kendra, a center dedicated to enhancing cyber security in the country. The Cyber Security Swachhta Kendra, also known as the Cyber Swachhta Kendra (CSK), was launched in February 2017 as a part of the Government of India's Digital India initiative. The term "Swachhta" translates to cleanliness in Hindi, reflecting the mission of the Kendra to ensure a clean and secure cyberspace for all users. The CSK operates under the guidance of the Indian Computer Emergency Response Team (CERT-In), which is the national agency responsible for responding to cyber security incidents and promoting a safe digital environment. The primary objective of the Cyber Security Swachhta Kendra is to provide a platform for effective coordination between various stakeholders in the field of cyber security. It acts as a hub for sharing information, best practices, and tools related to cyber security. The Kendra collaborates with government agencies, industry partners, academia, and users to identify emerging threats, develop mitigation strategies, and raise awareness about cyber security among the general public.

National Cyber Security Coordination Centre (NCCC)

The National Cyber Security Coordination Centre (NCCC) is a specialized agency established by the Government of India to serve as a central coordination point for cybersecurity efforts in the country. The NCCC operates under the purview of the Indian Computer Emergency Response Team (CERT-In), which is the national nodal agency for responding to cybersecurity incidents. The primary role of the NCCC is to monitor, analyze, and respond to cyber threats and incidents at the national level. It acts as a hub for collecting and sharing cyber threat intelligence, facilitating coordination among various government agencies, industry sectors, and other stakeholders involved in cybersecurity.

International Cooperation - Strengthening Global Defences

In today's interconnected world, where cyber threats transcend national boundaries, international cooperation in cybersecurity has become imperative. As digital networks extend across the globe, collaboration between nations has become essential to combatting cyber threats effectively. International cooperation in cybersecurity also extends to public-private partnerships (PPPs). The private sector plays a critical role in cyberspace, and collaboration between governments and industry can enhance cybersecurity efforts.

References

1. Akanksha Verma; Ragasree Surendra; B.Srikanth Reddy,Cyber Security in Digital Sector, Coimbatore, Mar.2021.
2. Deepa.T.P ; Survey on need for Cyber Security in India Publisher, Research Gate International Journal of Advanced Research in Computer and Communication Engineering, Vol,7,Issue 11,No.2018.

3. Kemmerer,Cybersecurity Proceedings of the 25th IEEE International Conference on Software Engineering,May, 2003.
4. Mallika; Vikas Deep; Purushottam Sharma, Analysis and Impact of Cyber Security Threats in India using Mazarbot Case Study,Belgaum,Dec.2018.
5. Md Iman Ali; Sukhkirandeep Kaur, The Impact of India's Cyber Security Law and Cyber Forensic On Building Techno-Centric Smartcity IoT Environment,Noida,Feb.2021.
6. Mohit Jain; Aryan Sinha; Aman Agrawal; Nimesh Yadav, Cyber security: Current threats, challenges, and prevention methods,Dehradun,Nov.2021.
7. Ramesh Subramanian, Historical Consciousness of Cyber Security in India,July.2020.
8. Rohit Chivukula; T. Jaya Lakshmi; Lohith Ranganadha Reddy, Study of Cyber Security Issues and Challenges,Gwalior,Nov.2021.
9. Sarvesh Tanwar; Thomas Paul; Kanwarpreet Singh, Classification and Impact of Cyber Threats in India: A review,Noida.Sep.2020.
10. Shailesh Khant; Atul Patel; Sanskruti Patel; Nilay Ganatra, Cyber Security Actionable Education during COVID19 Third Wave in India,London,April.2022.

Books

1. Amoroso, Cybersecurity, Newjersey,2006.
2. Lewis, Cybersecuity and Critical Infrastructure Protection, Washington, 2006.