CYBER SECURITY: A GROWING CONCERN IN TODAY'S DIGITAL LANDSCAPE

ABHINANDAN GHOSH

ASSOCIATE, A.C. BHUTERIA & CO.
CHARTERED ACCOUNTANTS

In today's digital era, cybersecurity has become an essential aspect of protecting individuals, businesses, and governments from cyber threats. With the rapid advancements in technology and increasing internet usage, cybercriminals have developed sophisticated methods to exploit vulnerabilities. This report delves into the importance of cybersecurity, its challenges, and the measures that can be taken to mitigate cyber threats.

Understanding Cyber Security

Cybersecurity refers to the practice of protecting systems, networks, and data from cyber threats such as hacking, malware, phishing, and data breaches. It involves implementing policies, technologies, and best practices to safeguard sensitive information from unauthorized access or attacks.

Key Components of Cyber Security

- **Network Security** – Protecting network infrastructure from unauthorized access.
- **Information Security** – Ensuring data confidentiality, integrity, and availability.
- **Application Security** – Securing software and applications from vulnerabilities.
- **Operational Security** – Managing security risks in business operations.
- **Disaster Recovery & Business Continuity** – Strategies to recover from cyber incidents.

Cyber Threats in Today's Age –

Types of Cyber Threats

I. **Phishing Attacks** – Fraudulent emails or messages to steal sensitive information.
II. **Malware** – Viruses, ransomware, and spyware that infect systems.
III. **Denial-of-Service (DoS) Attacks** – Overloading systems to disrupt services.
IV. **Man-in-the-Middle Attacks** – Intercepting communications to steal data.
V. **Zero-Day Exploits** – Targeting unknown vulnerabilities in software.

Some Stats-

Growing Cyber Threat Landscape in India: India has seen a significant rise in internet users, with over 750 million internet subscribers as of 2024. This digital revolution, while bringing immense opportunities, has also led to an increase in cyber threats. Cybercriminals are targeting businesses, government institutions, and individuals with increasingly sophisticated techniques. These threats include malware attacks, ransomware, phishing scams, and data breaches, which can have devastating consequences on both the financial and reputational fronts. A report from the Indian Computer Emergency Response Team (CERT-In) revealed that India witnessed more than 14 million cyberattacks in 2022 alone, a stark reminder of the vulnerabilities that exist in the country's digital infrastructure. As India continues to embrace digital transformation, the country's dependence on the internet and technology grows exponentially. This rise in digitalization, however, has also made India a prime target for cybercriminals. Cyberattacks have become more frequent, sophisticated, and damaging in recent years, impacting individuals, businesses, and government organizations alike. From financial frauds to data breaches, the threat landscape in India is increasingly complex.

Cyber-attacks in India in the recent past

- **AIIMS Delhi Ransomware Attack (2022):**

  Background

  On November 23, 2022, AIIMS experienced a severe ransomware attack that disrupted its hospital management system (HMS) and electronic health records (EHR). These systems were crucial for managing patient appointments, medical records, and diagnostics, and their failure caused major delays in medical treatments and surgeries. The attackers encrypted hospital data and demanded a ransom for decryption keys, though the exact amount was not disclosed. The attack left AIIMS locked out of its own systems, making critical patient records inaccessible and disrupting healthcare services.

  Impact & Response:

  The attack paralyzed critical hospital operations, making patient data inaccessible and delaying treatments. CERT-In and I4C were alerted, and cybersecurity experts were deployed to investigate and recover systems. AIIMS did not confirm if ransom was paid, but recovery was long and complex.

Key Takeaways:

Healthcare Vulnerability – Hospitals with sensitive data are prime targets for cyberattacks.

Need for Backups & Disaster Recovery – The attack emphasized the importance of strong backup systems to prevent disruption.

Government & Cybersecurity Preparedness – Though the Indian government responded quickly, the incident exposed gaps in cybersecurity infrastructure in critical sectors.

This attack highlighted India's healthcare cybersecurity challenges and the urgent need for better defences against ransomware threats.

- **Star Health Data Breach (September 2024):**

Background

Star Health, India's largest health insurer, experienced a data breach where a hacker leaked customer information, including medical records and personal identification details, via Telegram chatbots. The hacker claimed to possess over 7 terabytes of data affecting more than 31 million customers.

Impacts

Personal and sensitive health information of over 31 million customers, including medical records, PAN numbers, and Aadhaar details, were leaked, leading to privacy and security risks.

The breach erodes customer trust, damaging Star Health's brand image and raising concerns over the company's data protection practices. Star Health may face regulatory penalties, lawsuits, and financial losses due to non-compliance with data protection laws (e.g., GDPR, India's Data Protection Bill).

Mitigations

Continuously monitor for leaked credentials that open a completely different Attack surface and validate those credentials on your infrastructure, Rigorous and frequent API testing should be done to check for data exposure flaws, Implement behavioural detection/rate limiting and MFA on customer login endpoints as well to avert credential stuffing attacks, Implement robust encryption for stored and transmitted data, along with regular security audits to identify vulnerabilities, Strengthen access management, including limiting privileged account access and implementing multi-factor authentication (MFA) for all employees and third parties. Keep an eye out for insider threats.

In 2020, the Aadhaar database, India’s national biometric identity system, was reportedly leaked. Although the government denied any breach, concerns over data privacy persist.

Cosmos Bank Cyber Attack (August 2018):

In August 2018, Pune's Cosmos Cooperative Bank was targeted in a sophisticated cyber-attack involving malware injection and unauthorized transactions. This breach led to significant financial losses due to unauthorized withdrawals from numerous accounts.

Global Cyber Attacks

- **WannaCry Ransomware Attack (2017) –**

Background

The WannaCry ransomware attack began in April 2017, exploiting a vulnerability in Windows SMB (Server Message Block) using the EternalBlue exploit, originally developed by the NSA. It spread rapidly across networks, encrypting files and demanding $300 in Bitcoin as ransom. The attack used a dropper to execute the ransomware, which checked for a specific unregistered domain—acting as a killswitch if found. If not, it proceeded with encryption, displaying a ransom note with two deadlines: a three-day window before the ransom doubled and a seven-day limit before permanent data deletion. The malware used RSA and AES encryption, making decryption nearly impossible without payment. However, due to poor coding, payments couldn’t be linked to victims, meaning paying the ransom didn’t guarantee file recovery. A ‘demo’ feature decrypted 10 random files to convince victims it was legitimate.

Impact:

WannaCry infected 250,000+ systems across 150 countries, making it one of the most widespread ransomware attacks in history.

Response:

But a kill switch was discovered by British security researcher Marcus Hutchins, who inadvertently stopped the attack by registering a web domain found in the malware's code. Once the ransomware checked the URL and found that it was active, it was shut down – buying precious time and giving organizations breathing room to update their systems.

- **Facebook Marketplace Database Leak (2023) –**

  Background

  The infamous threat actor known as IntelBroker has claimed responsibility for leaking a partial database of the Facebook Marketplace. The alleged breach, apparently conducted by another cybercriminal using the alias "algoatson" on Discord, occurred in October 2023. However, the database was only made public earlier today, on Sunday, February 11, 2024.

  According to a post on Breach Forums, IntelBroker disclosed that the hack targeted a contractor responsible for managing cloud services for Facebook. The breach resulted in the theft of approximately 200,000 entries from the user database, compromising sensitive personal information. It is worth noting that IntelBroker did not disclose the name of the allegedly targeted contractor. Facebook doesn't utilize a single contractor company to manage all of Facebook Marketplace data. Instead, they leverage a combination of internal teams and external partnerships depending on the specific data aspect. The compromised data includes full names, Facebook IDs, phone numbers, physical IDs, and Facebook profile settings of the affected users.

How can users protect themselves?

i. Change Passwords and Enable Two-Factor Authentication (2FA)

ii. Monitor Account Activity: such as unrecognized logins or changes to account settings. Report any unauthorized activity to Facebook immediately.

iii. Be Cautious of Phishing emails, messages, or calls pretending to be from Facebook or other trusted sources. These may attempt to trick users into revealing sensitive information or clicking on malicious links.

iv. Review and adjust Facebook privacy settings to limit the visibility of personal information. Additionally, consider locking Facebook profile if the feature is available in one's country.

v. Watch Out for Voice and SMS Phishing and if we get a call or text asking for sensitive stuff like bank details, do not disclose the same. Also don't click on any links or reply if not sure who it's from.

Importance of Cyber Security

With the increasing digitalization of services, cyber threats pose significant risks to individuals and organizations. Key reasons why cybersecurity is crucial include:

- **Protection of Sensitive Data** – Preventing data leaks and unauthorized access.
- **Financial Security** – Avoiding financial losses due to fraud and cybercrimes.
- **National Security** – Safeguarding critical infrastructure from cyber warfare.
- **Trust and Compliance** – Ensuring customer trust and adherence to regulations.

Cyber Security Measures and Best Practices

i. **Personal Cyber Security Measures**- Use strong, unique passwords and enable multi-factor authentication (MFA), avoid clicking on suspicious links or downloading unknown attachments, keep software and antivirus programs updated, be cautious of public Wi-Fi networks.

ii. **Organizational Cyber Security Strategies**- Implement robust firewalls and intrusion detection systems, educate employees on cybersecurity awareness and phishing detection and develop an incident response plan for quick mitigation of cyber threats.

Cyber Security Laws and Regulation

Governments worldwide have introduced various laws to enhance cybersecurity. Some notable regulations include:

- General Data Protection Regulation (GDPR) – EU
- Cybersecurity Information Sharing Act (CISA) – USA
- Information Technology Act, 2000 – India
- NIST Cybersecurity Framework – USA

These regulations help in enforcing strict security policies and protecting consumer data.

Conclusion

Cybersecurity is a critical concern in today’s interconnected world. The increasing sophistication of cyber threats requires individuals and organizations to stay vigilant and adopt strong security practices. As technology continues to evolve, the need for enhanced cybersecurity frameworks, awareness, and proactive measures becomes even more crucial. By implementing the right strategies, we can build a more secure digital environment for the future.