IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, Iss 08, 2022

Cybersecurity Issues and Approaches in India's Different Sectors

Asst. Prof. Supriya T. Mali
Department of Computer Science
Sonopant Dandekar Shkshan mndali, Palghar (W), Maharashtra, India.

Abstract:

The speedy digitization of services and transactions have made cybersecurity a top priority for India's banking and government sectors. This study looks at these industries' cybersecurity issues and suggests ways to strengthen their defenses against online attacks. This paper emphasizes the urgent need for strong cybersecurity measures through a thorough review of the present landscape, regulatory framework, and case studies of recent cyber-attacks. India can preserve sensitive data, maintain national security, and increase confidence in its digital infrastructure by successfully tackling these issues.

Keywords: Cyber Security, cyber-crime, data protection, Preventive measures

Introduction:

The way we live and work has changed dramatically in the past year due to the broad acceptance of digital technology and its expanding reach. Undoubtedly, the digital revolution has brought numerous advantages; but, it has also revealed the dark area of cybercrime. Sadly, there has been a concerning increase in cybercrime activity even in areas that were previously unaffected by this threat.

Strong cybersecurity protocols are important particularly in India, where the banking and government sectors play a pivotal role in the nation's economy and governance. This introduction looks at the complicated landscape of cybersecurity concerns affecting different sectors in India and provides strategies for boosting defenses against new cyberattacks.

India, like many other nations, is experiencing an increase in cybercrime in 2018, 208,456 cyber-related offenses were reported. More cybercrimes were reported in the first two months of 2022 than there were in the whole of 2018.

Even more sharply growing numbers were recorded during the epidemic: from 394,499 cases in 2019 to 1,158,208 cases in 2020 and 1,402,809 offenses in 2021, the numbers rose even more. India had a 15.3% rise in cybercrime between Q1 and Q2 of 2022. In addition, the number of Indian websites that have been hacked in recent years has been rising. 18,560 or so websites were compromised in 2018. A total of 26,121 sites experienced hacking in 2020.

In 2021, ransomware attacks affected 78% of Indian organizations, and in 80% of those cases, data encryption was the outcome. As compared to this, the average encryption rate was 65% and the average percentage of attacks was 66%.

Significant Data Leak at Covid Time:

The data breach described involves the leakage of sensitive information from thousands of Indian citizens who registered on the COWIN application for COVID-19 vaccination. This breach is significant for several reasons.

The leaked data includes a variety of personally identifiable information (PII) such as names, dates of birth (DOB), gender, phone numbers, Aadhar details, passport details, and the location where the first dose of the COVID-19 vaccine was administered. The inclusion of DOB is particularly concerning as it can be used for various purposes beyond just identification.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, Iss 08, 2022

Given the widespread use of Aadhar details for various services in India, the leak of such comprehensive data exposes individuals to potential identity theft, financial fraud, and other malicious activities. Additionally, the leakage of passport details can pose a security risk for affected individuals, especially regarding international travel and related services.

The existence of multiple copies of the leaked database increases the risk of misuse, as anyone with access to the database can perform reverse queries based on mobile numbers. This raises concerns about the accessibility of personal information to unauthorized parties and the potential for exploitation.

The inclusion of DOB in the leaked data enhances the potential for resetting passwords and gaining unauthorized access to various online accounts linked to individuals' personal information.

Cyber Crime in Various Sector:

a) Government Sector:

Keeping sensitive data and vital infrastructure safe from cyberattacks is a problem for governments. Cybercrime has increased as a result of the quick development of technology, growing interconnectedness, and digitization of many industries. The increased dependence of individuals and companies on digital platforms and their massive data storage on these platforms raises the potential for cybercriminals to launch attacks and exploit weaknesses.

Compared to the commercial sector, the government saves significantly more data and does so for longer periods of time, which makes its systems more vulnerable. And as governments attempt to fortify themselves against outsiders, workers and citizens alike desire easy access to their data.

A cyber security firm, RESECURITY has reported a major data leak involving personal information of over 81.5 crore (815 million) Indians. This data allegedly sourced from the indian council of medical research (ICMR), has been found on the dark web and includes names, phone number, addresses, aadhar and passport information. A threat actor known as ‘ pwn0001’ broked access to this data , offering the entire aadhar and indian passport database for $80,000.

In response to the growing menace of cybercrime, governments across have enacted laws and formed specialized law enforcement units and cybersecurity agencies. The aforementioned procedures are designed to discourage cybercriminals, look into cybercrimes, and make sure the people who commit them are held responsible.

b) Banking:

Year 2020 has proven to be a difficult year for Indian banks in terms of cybersecurity. Banking operations had significant disruptions following the start of the COVID-19 pandemic, as banks found it difficult to continue serving their customers while under various lockdown phases. To guarantee frictionless company operations, they stepped up their digital transformation initiatives in the ensuing months (including digital banking and staff remote access). As banks saw a rise in digitalization, hackers also saw an increase in attacks since they were able to take advantage of new openings and weaknesses.

Banks will need to strengthen their cyber defense operations in order to meet stakeholder expectations, avoid risks, and comply with regulatory obligations in order to remain relevant and competitive. Banks can anticipate more frequent and advanced attacks as they concentrate more on shifting resources to digital platforms. Attacks against end users' computing environments will move from in-house devices to those hosted on digital platforms that are accessed by various stakeholders. Banks will need to manage end-user education, regulatory compliance, and proactive measures to address cyber risks arising from multiple security aspects, including data, application, identity, infrastructure, and cloud . They must continually close

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, Iss 08, 2022

security holes, create a security roadmap, evaluate and compare best practices, and decide on strategic investments in cybersecurity's key areas.

Preventive Measures for Consumers:

1. Consumer can use strong and unique password.
2. Consumer should on two factor authentication by adding extra layer of security.
3. Consumers should be alert while clicking on email and link if they are getting from unknown source.
4. Consumer should update software and devices regularly.
5. Consumers should check their bank statement and account detail regularly.

c) Mobile Industry:

As Devusinh Chauhan , minister of state of communication told to parliament , As on Dec 13, Results of the SANCHAR SAATHI portal include the disconnection of 55.52 lakh mobile connections obtained through fraudulent or fake documents, the blocking of 1.32 lakh mobile phones for their potential involvement in financial fraud or cybercrime, and the disconnection of 13.25 lakh suspected citizen-reported mobile connections that did not pass re-verification, 67,000 dealers SIM activated, 300 FIR register for the same 66000 WhatsApp account are blocked because Fraud messages and Fraud call were started receiving.

A Central Equipment Identity Register ["CEIR"] is a centralized database of mobile equipment identifiers (i.e. IMEI for networks of GSM standard) statistics has given the region those who are having high no. of cases. (Top 10)

SR No.	Location	Mobile Blocked	Mobile Traced	Mobile recovered
1	NCT Delhi	4,90,848	2,96,271	2,377
2	Karnataka	1,97,380	82,471	26,984
3	Maharashtra	1,82,649	89,053	11,350
4	Andhra Pradesh	34,708	16,715	5,267
5	Punjab	29,450	15,889	1,164
6	Haryana	18,038	9,389	1,205
7	Chhattisgarh	18,029	10,323	2,056
8	Kerala	16,148	8,683	1,595
9	Madhya Pradesh	15,049	7,832	1,069
10	Bihar	14,421	8,531	855

d) Pensioner:

Around 28 crore Indian pensioners have had their information compromised because of data leak.

The Digitalized pension processing system, **SPARSH (System for pension administration Raksha)** developed by TCS suffered a data breach in this year. **SPARSH** offers online pension related facilities to over 3 million pensioners from 50 organization. Sensitive information such as usernames, passwords, ULRs, pension numbers, and more was leaked from the SPARSH portal. Reports that data from the SPARSH data dump is also being sold on a Russian marketplace have sparked concerns about the possible involvement of Russian hacker groups. It is believed that the malware known as "lumma" is to blame for the 0.41 million bytes of exposed data that were sold for nine dollars.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, Iss 08, 2022

e) To elder people:

3500 cases of cyber fraud are reported daily across India, with senior citizens targeted the most. Due to their ignorance of digital products, seniors are more vulnerable to cyber fraud in the digital age.

Problem of Cybercrime against Elderly:

a) Through Stranger :

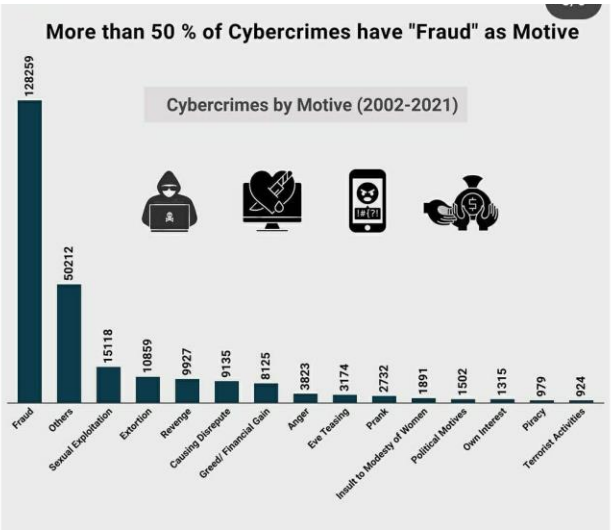
- Investments: Since a large number of seniors are on fixed incomes, they frequently wish to enhance the value of their inheritance and make sure they have enough money to cover their essential expenses. In investment scams, fraudsters use false high rates of return to attract elderly victims into investing in stocks and bonds, real estate, precious stones, or annuities. Often, the investments are made up of phony jewels, uninhabitable real estate, or stock in a business that is either bankrupt or nonexistent.
- Loans and mortgages: seniors who require home maintenance or medical care may find themselves short on funds. Criminal lenders frequently put elderly borrowers' properties at risk by offering loans with excessive interest rates, undisclosed costs, and repayment plans.
- Charity contributions: Taking advantage of seniors' humanitarian tendencies, criminals raise money for bogus charities or religious institutions, frequently by holding raffles or prizes.

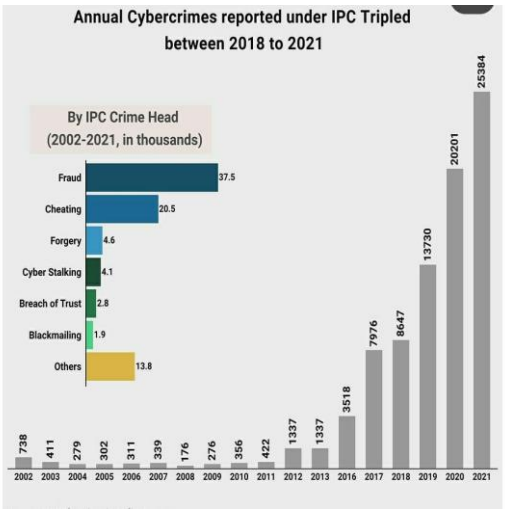
b) Financial Abuse by Family Members and Guardians: They misuse of their relationship with elder people by taking their money and not paying back and by misusing their Debit and Credit card.

Seven-step recommendations to address cyber threats:

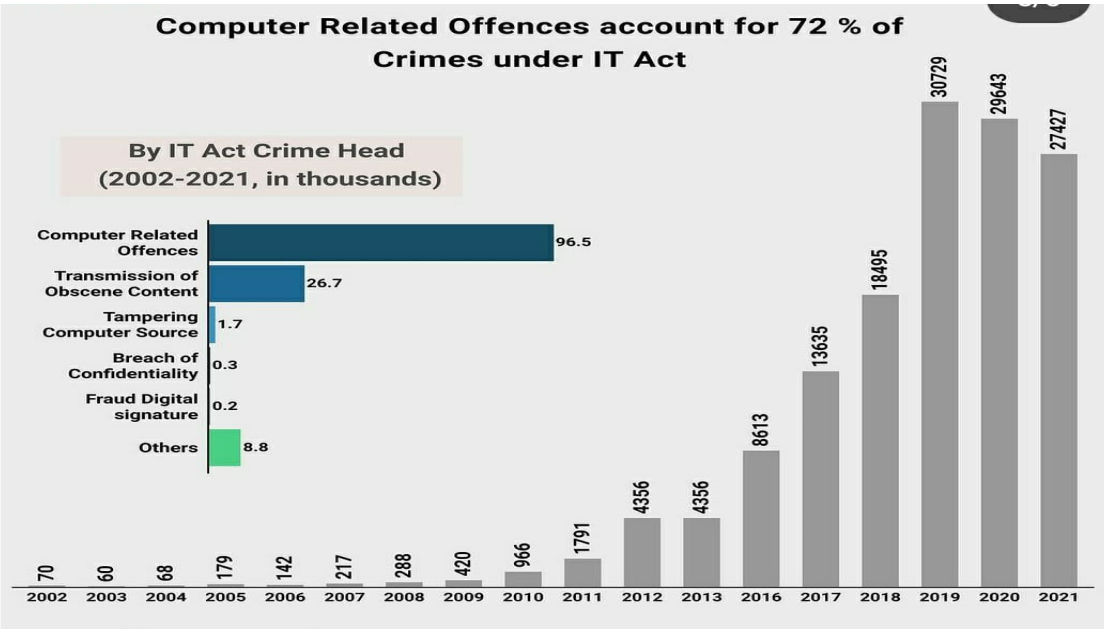
These recommendations are not exhaustive but essential to ensure robust security and compliance.

1. Prioritizing cybersecurity assessment
2. Securing remote access control
3. Tightening access to third-party services
4. obtaining cybersecurity skills through outsourcing or contracting
5. Implementing cutting-edge technological tools and solutions
6. Increasing attention via instruction
7. Enhancing security by using threat detection and response skills





ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, Iss 08, 2022



Conclusion:

India needs to create a thorough cybersecurity policy that defines national cybersecurity objectives and sets industry-wide cybersecurity standards. The policy should provide instructions for recovering from incidents and responding to them. To detect and reduce cybersecurity concerns, the Indian government should collaborate closely with business. This could include forming working groups focused on cybersecurity within particular industries and forming public-private partnerships to develop cybersecurity solutions. It is also explained how cyber-crime happens in different sector what are the preventive measures for consumers.

References:

https://heinonline.org/HOL/LandingPage?handle=hein.journals%2Flwsfkhv2023&div=46&id=&page=
https://sancharsaathi.gov.in/
https://www.business-standard.com/india-news/govt-pension-portal-for-defence-personnel-sparsh-suffers-data-breach-124011000128_1.html
https://www.varindia.com/news/data-leak-of-pension-portal-puts-indian-defense-personnel-at-risk
Knowledge-of-Cybercrime-among-Elderly.pdf
Introduction to the Concept of IT Security.pdf
in-ra-cybersecurity-in-the-indian-banking-industry-noexp (1).pdf
Cybersecurity in government of India.pdf
https://www.thequint.com/fit/cowin-data-breach-private-information-covid-vaccine-telegram-bot
Bick B.J. (2011), "Internet crime and the Elderly", New Jersey Law, 2(4):1-2
Campbell R.J. & Wabby J. (2003), "The Elderly and the Internet: A case study", The Internet Journal of Health, Vol.3, Issue.1