

## **Banks on Cybersecurity**

### **What is the issue?**

As the world goes on to connect more and more digitally, infiltration of cybercriminals have been increasing pushing the need for stringent cybersecurity measures for digital banking.

*India was the second most cyber-attacked country in Asia-Pacific in 2020, a new study by technology major IBM has revealed. India is now ranked at No. 10 on the Global Cyber Security Index, up from No. 47 in 2019*

### **What are the threats of digital banking?**

- **Malware** - Devices infected with malicious software pose a serious security risk to the bank's cyber security network, whenever they connect with it.
- **Third-party services** - Numerous financial institutions employ the services of third-party vendors to serve their customers in a better manner which is an easy target for cybercriminals.
- **Spoofing** - Cybercriminals try impersonating a bank's URL with a website that is quite similar to the original one(fake website) to steal the credentials.
- **Phishing** - Attempt to obtain sensitive information such as credit card details for fraudulent activities, by disguising oneself as an authentic, trustworthy entity via electronic communication are known as phishing.
- **Unencrypted data** - whatever data that is stored on the computers, servers or the cloud if unencrypted becomes a gateway for cybercriminals.
- **Denial of Service (DoS)** - blocking access to websites

## RECENT DATA BREACHES

2.5 mn

**Airtel:** Name, DoB, phone numbers, address, Aadhaar. Up for sale for bitcoins worth \$3,500

3.5 mn

**MobiKwik:** KYC info

20.0 mn

**BigBasket:** Personal information, address, PIN, IP addresses, etc for sale for \$40,000

22.0 mn

**Unacademy:** User name, password, and email

35.0 mn

**Juspay:** Masked card data & card fingerprint data was for sale for \$5,000 Bitcoins

Source: News reports

### What are the challenges in ensuring cybersecurity?

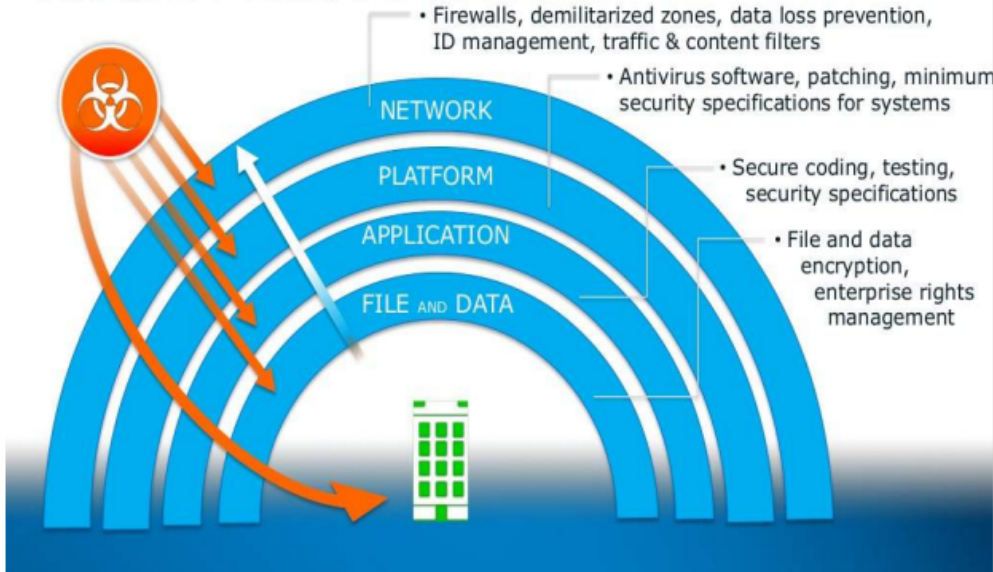
- **Lack of awareness** - Digital illiteracy and lack of awareness about cybersecurity is a challenge.
- **Increased use of social media** - With the advent of social media and its increased adoption, hackers have learned to exploit the medium.
- **Inadequate budget and lack of management** - Budgetary allocations to cybersecurity is often neglected.
- **Weak identity and access management** - Issues such as one hacked credential can give a hacker access to the entire enterprise network.
- **Increase in Malware** - Recent incidents of Pegasus spyware, malware attacks on kudankulam power plant, Colonial Pipeline Cyber Attack, etc. are notable examples for their rise.

### What are the solutions to address the issue?

- Integrated security with multiple layers become crucial for regulated sectors like Banking, financial services and insurance (BFSI) as various elements can work and communicate together.

# Tactical Security Technology Integration: Layered Defense

Multiple layers are necessary for comprehensiveness



- Data analytics and machine learning are essential for leveraging smart security solutions which aids BFSIs to store and assess high volumes of security-related data in real-time.
- Updated antivirus and anti-malware applications offer best protection from potentially disastrous attacks.
- Financial institutions need to invest in technologies that can enhance the endpoint protection.
- A fool-proof cybersecurity system, that doesn't compromise with data pertaining to customers and financial institutions has to be the primary focus for a rapidly digitising BFSI system.

**Source: Business Line**