ManageEngine
Endpoint Central

Cybersecurity priorities of the Indian banking industry post pandemic

Table of Contents

Introduction

Wrestling with a pandemic and its lasting effects has caused major turbulence among various industries in India. And in times of turbulence, cybercriminals thrive. Asia moved to first place on the list of the most attacked regions in 2021, encountering 26% of all attacks, of which Japan, Australia, and India were the biggest targets in Asia.

With the majority of cyberattacks aiming to steal money, what better money stockpile to attack than banks? Naturally, the banking sector has become the sector most targeted by cyber criminals. As reported by the IBM Security X-Force Threat Intelligence Index, in 2021, finance and insurance organizations faced the highest number of cyberattacks, making up 30% of total incidents, followed by the manufacturing and professional service sectors.

Gone are the days when burglary and robbery were the biggest threat to banks. Today, the banking sector is especially vulnerable to cyberattacks for two reasons: its monetary holdings and the value of the data it possesses. When it comes to the banking sector, cybercrimes don't stop at causing a lack of access control or system downtime but have grown to cyberswindling, like stealing credit or debit card data, siphoning money through infected ATMs, and designing sophisticated software to launder money and cover their tracks.

Given the ever-evolving sophistication of cybercriminals and their attacks, you need to stay one step ahead of them to safeguard your network and your business.

The Four Worst Cyberattacks In The Indian Banking Industry

2016

India's Largest Data Breach

Malware Attack

Data regarding about 3.2 million debit cards was compromised from various banks across India, including State Bank of India (SBI), HDFC Bank, ICICI Bank, YES Bank, and Axis Bank. Attackers achieved this by injecting malware into the payment service systems hosted by Hitachi Payment Services. Cybersecurity company SISA analyzed and confirmed that the malware stole both the debit card number and the PIN of affected customers. In light of this, the biggest Indian bank, SBI, announced that it would block and re-issue almost 600,000 debit cards[2], and the other affected banks followed suit. This stands to be the biggest data breach till date in the history of the Indian banking sector.

2017

Union Bank Of India Hacked

Phishing

The attack was initiated when an employee of Union Bank of India fell prey to a phishing email that was made to look like an email from an Indian central bank. This email contained an attachment with malicious code that, when opened, initiated a malware attack and allowed the hackers to access the bank's network and steal the bank's access codes for the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT being a service used for international transactions, the attacker then proceeded to transfer $170 million to a Citigroup account in New York.[3]

2018

UIDAI Aadhaar Software Hacked

Corrupted Patch

The Indian government's unique identification software UIDAI Aadhaar was hacked using a patch that disabled critical security measures. As much as patches can fix vulnerabilities, they can also be used to introduce vulnerabilities into software. It all started when, back in 2010, the UIDAI permitted private agencies to enroll users in the Aadhaar software in order to accelerate the enrollment process. The enrollment operators were required to log in by first scanning their fingerprint or iris while a GPS feature in the software verified their location. A malicious patch was introduced that disabled the built-in security measures, bypassing the need for authentication, disabling the software's built-in GPS, and reducing the accuracy of the iris recognition feature. This set into action a series of offenses, including attackers bypassing authentication of enrollment operators and creating ghost entries in the Aadhaar database, hacking around 210 Indian government websites[4], and breaching sensitive data like Aadhaar numbers, PANs, IFSC codes, iris scans, fingerprint scans, and other personal information of the software's users.

2018

Cosmos Cooperative Bank Attack

Cosmos Cooperative Bank reported a two-day malware attack on its ATM bank servers that siphoned off Rs 94.42 crore through online transfers and ATMs.[5] On August 11, 2018, numerous debit cards of Cosmos Cooperative Bank customers were cloned, and around 15,000 ATM transactions were made from India and 28 other countries in a time span of seven hours, laundering Rs 80.5 crore.[6] The next day, another 13.92 crore were transferred to a Hong Kong-based firm using SWIFT.

Malware Attack

Major IT Threats Faced Today

Malware

Malware continues to be the biggest threat to the banking industry, with there now being easier access to malware technology than ever. Any device that is part of the network, either for everyday use or for performing sensitive operations, can end up posing a serious security risk to a bank's cybersecurity network. Businesses encountered 50% more attacks per week in 2021 compared to 2020.[7] The Log4j vulnerability was one of the major contributors to this threat in 2021.[9]

Phishing

Attempting to obtain sensitive data such as credit or debit card details, CVV numbers, and ATM PINs by distinguishing oneself as an authentic entity via online communication is known as phishing. As our digital footprint has increased, so has the frequency of bank phishing scams. The 2021 Verizon Data Breach Investigations Report noted that 32% of all data breaches result from phishing emails.[10]

Spoofing

For the past four years, spoofing has gradually grown to be a serious concern in the banking industry. Cybercriminals impersonate a bank's web address with a fake URL and redirect a user to log in to the fake website so the attacker can steal their credentials. Spoofing can cause major reputational and financial damage to banks.

Unencrypted data

It is important that whatever data is stored on an organization's systems or servers be fully encrypted. This way, in the event of a data breach, cybercriminals will not be able to use the data to cause any further damage.

- **Lack of end-user awareness**

Unlike traditional attacks that exploit software vulnerabilities, lack of end-user awareness has given the scope for social engineering attacks that exploit human weaknesses. An Infosec report revealed that, in a survey conducted, 97% of users could not distinguish between a phishing email and a legit one.[8]

- **Weak identity and access management**

One of the fundamental elements of cybersecurity is identity and access management, which many organizations still struggle with. In an era where hackers seem to have the upper hand, it requires only one hacked credential to gain entry into an enterprise network and encrypt the organization's data, locking out the rightful authorities.

- **Mobile devices and apps**

Apps have become the pulse of the planet, and since financial transactions are now increasingly being done on banks' mobile apps, the mobile phone is becoming an appealing target for malware deployers. Jailbroken and rooted devices increase the scope of attacks when used for banking.

The Digital India Initiative's Impact On Cybersecurity

In 2015, the Indian government launched the Digital India initiative, which aims to bridge the digital divide in India by bringing in e-governance and digital finance with schemes such as DigiLocker, Aadhaar, BharatNet, BHIM, MyGov, e-Health, e-Education, and public Wi-Fi. Digitization surely brings unmatched functionalities, coverage, and usability for the large Indian population. However, it has also brought in a fresh batch of cyber risks.

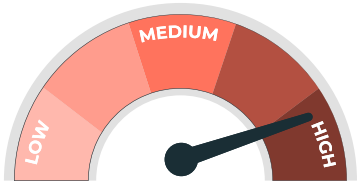
With the entire country going digital, taking every security measure possible is important to protect data and privacy. The digital transformation of the banking industry with mobile apps, online banking, and other online services has left this industry vulnerable to more attacks.

It's understandable that higher digitization and remote operations will lead to increased vulnerabilities and open up opportunities for cybercriminals.

The pandemic's effect on cybersecurity

After COVID-19 was declared a pandemic and a lockdown was announced country-wide, finance operations in India were severely interrupted as banks struggled to provide uninterrupted services to customers while keeping themselves up and running.

An overnight push to remote operations led to increased vulnerabilities and opened up new opportunities for cybercriminals. Like every sector, banking was hit hard by the pandemic, if not the hardest. Below is how the pandemic affected the cybersecurity of the banking sector:



High Risk Category

The Reserve Bank of India (RBI) reported that for the first time since the inception of its systemic risk surveys, cyber risk appeared in the "high risk" category. The survey, which lists major risks faced by the financial system, was conducted between April and May 2020, after the COVID-19 lockdown.[11]

Around 66% of Indian organizations suffered at least one data breach after shifting to the remote work model during the pandemic lockdown.[12] Fifty-five percent of surveyed organizations reported a data breach in which credentials were stolen, and 44% stated that misconfigurations in open ports attracted attacks on their companies.[12]

Increase in Data Breach

Increase in Cyberattack

As reported by cybersecurity firm Sophos, about 93% of Indian organizations suffered a cyberattack within a year after the pandemic began.[13]

In research conducted by Deloitte, BFSI cyberattacks increased 238% between February 2020 and April 2020.[14]

Increase in Cyberattack

40,000+

Hacker Attempts

About 40,000 cyberattacks on India's IT and banking industry were attempted by hackers around the globe in the last week of June 2020.

According to a study by IBM Security, the average total cost of a data breach in India reached Rs 14 crore in 2020, which is an increase of 9.4% from 2019. And the average time taken to curb a data breach increased from 77 days to 83. This cost comes to Rs 5,522 for a single hacked credential, which is an increase of 10% from 2019.[15]

14 Crores

Cost of Breach

The Indian Government's Response To Growing Cybercrime In The Finance Sector

1. Reserve Bank Information Technology Pvt. Ltd.

The Reserve Bank of India (RBI) has set up Reserve Bank Information Technology Pvt. Ltd. (ReBIT) to take care of the bank's IT needs, including the cybersecurity aspects of RBI. ReBIT will mainly focus on strengthening the cybersecurity of the financial sector in India and assist in IT system audits as well as assessments of RBI-regulated entities. Below are a few initiatives undertaken by ReBIT to benefit the Indian banking sector:

Community Leadership

ReBIT works with industry experts to implement initiatives that strengthen the cybersecurity of the financial sector.

Cybersecurity Maturity Model Working Group

This maturity model is a product of ReBIT's tie-up with the banking CISO community. This model allows service providers and stakeholders to assess a company's preparedness using tested and approved metrics.

Cybersecurity Assessment Framework Working Group

This working group works on defining a cybersecurity assessment model for financial organizations.

Operational Excellence

This initiative of ReBIT comprises a series of webinars that educate administrators or security practitioners in the financial industry on case studies, best practices, and the latest tools and technologies for staying updated.

Periodic Newsletters on Cybersecurity

The readership of this newsletter is aimed at the people in the top stratum of leadership would be able to influence the happenings around cyber security policies within their organizations positively.

2. Computer Emergency Response Team for the financial sector

The government of India has introduced a Computer Emergency Response Team for the finan-cial sector (CERT-Fin). As stated in the Working Group on Digital Lending's report, CERT-Fin will gather, analyze, and distribute necessary information on cyber incidents in the financial sector. It will coordinate and take emergency action around cybersecurity incidents when the need calls for it, and will also send alerts on any possible cybersecurity incidents.

Six Things To Do Better Post Pandemic

1) Employee education

Your organization is only as secure as each of your employee's cybersecurity awareness. Employees remain the first line of defense for an organization, and it is important that they know the role they play in protecting the organization. They must be trained to discern the consequences of their actions, and the response strategy in case of an incident. Banking firms must invest in regularly training and improving the cybersecurity awareness among their employees.

2) Penetration testing

Familiarity breeds contempt; similarly, getting used to your organization's ways may lead you to overlook a few obvious security flaws. That is why an external pair of eyes is necessary to give you fresh insight into everything that is wrong with your network. The first step towards building strong protection for your network is being aware of the weaknesses in your company's online systems so you can remediate them. Penetration testing is a great way to analyze weaknesses, strengthen defenses, and remain compliant with the necessary standards. Through robust pentesting, you can close loopholes and build an optimal cybersecurity program.

3) Continuous assessments

Security is not a one-time job, but everyday work. Conducting security checks will often misconfigured devices, defective security policies, outdated software versions, or vulnerabilities in third-party applications. Big breaches usually stem from a small misconfiguration. With the increasing adaptation to a remote workforce, the need for organizations to keep their networks well-groomed is greater than ever. A bank's operational needs and cybersecurity needs need to level up to the same importance for continued protection from cybercriminals.

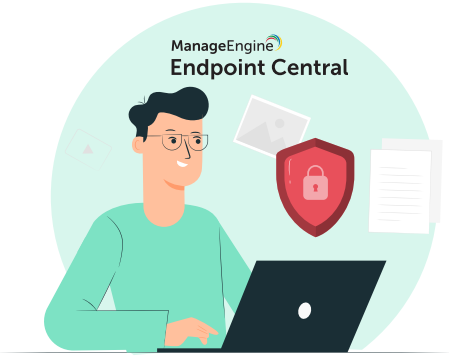
4) A dedicated cybersecurity team

Banking firms need to understand that security is not an additional cost but a necessary investment. Even though cybercrimes are fought with technology, it is people who run this technology. It is important to build up a team of professionals who are equipped and trained to tackle the threats of today's times. Allocate a budget to create a dedicated cybersecurity team that can regularly probe the security state of the company.

5) A foolproof incident response plan

As popularly said, it is not a question of 'if' an organization will be attacked, but 'when'. Organizations need to prepare for the worst while hoping for the best. It is important to be ready to face such attacks and not only respond but effectively recover with as little damage as possible.

6) Next-gen endpoint protection



The traditional way of managing an organization's endpoints is no longer enough on its own in light of today's range of threats. Banks and other financial institutions must invest in software that uses next-generation technology that can effectively identify, manage, and secure a network's endpoints right from their onboarding and up until their retirement. A unified endpoint management solution is essential to manage and secure the different types of devices in your network, like desktops, laptops, mobile devices, printers, and scanners, from a single platform. ManageEngine's unified endpoint management solution Endpoint Central can help you increase the cyber resilience of your company.

How ManageEngine Can Help

Having been a key player in the market for more than 20 years, ManageEngine offers IT management and security solutions for any possible requirement you'd have for managing a company's endpoints. With robust capabilities and usability, ManageEngine simplifies and automates the process of managing and securing your network, all from a single console. It offers visibility, control, and security from the comfort of your desk, along with seamless integrations among products that serve different operational needs.

ManageEngine's endpoint management solution, Endpoint Central, is a powerful UEM solution that manages devices like servers, desktops, laptops, and mobile devices from a single dashboard and supports OSs like Windows, macOS, Linux, iOS, Android, Windows, tvOS, Chrome OS, and iPadOS. You can perform **End-to-End Patch Management, Remote control, Asset Management, OS Deployment, Mobile Device Management, Configuration Management, and Security Operations, including Vulnerability Management, Browser Management, Application Control, Device Control, and BitLocker Management.**

Visit ManageEngine's UEM page.

Find us on Gartner peerinsights Capterra G2

sales@manageengine.com | +1-925-924-9500

Follow us on

References

1. https://www.ibm.com/downloads/cas/ADLMYLAZ

2. https://www.livemint.com/Industry/jVF2Aw72w0DcBsUGseV0UP/Malware-caused-Indias-biggest-debit-card-fraud-Audit-repor.html

3.https://www.firstpost.com/tech/news-analysis/recent-cyber-attack-on-union-bank-in-india-was-similar-to-the-hack-attack-in-bangladesh-cyber-heist-3700825.html

4. https://www.firstpost.com/tech/news-analysis/uidai-aadhaar-software-hacked-using-a-patch-which-disabled-critical-security-report-5159521.html

5. https://www.reuters.com/article/cyber-heist-india-idUSL4N1V551G

6. https://www.hindustantimes.com/cities/15-months-later-no-lead-in-rs-94-cr-cosmos-bank-cyber-fraud-case/story-Ar6lk69HLJmBEyt9jGsx0K.html

7. https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/

8. https://resources.infosecinstitute.com/topic/security-awareness-statistics/

9. https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf

10. https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-dbir-2021

11. https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1179

12. https://www.livemint.com/technology/tech-news/cyberattacks-hit-93-indian-organisations-in-last-one-year-11594635863531.html

13. https://www.sophos.com/en-us/medialibrary/gated-assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

14. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-in-the-indian-banking-industry-noexp.pdf

15. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic